Contents

UPS Menu 90

Environment Menu 136

Event-Related Menus 141

Data Menu (Web Interface Only) 160

Boot Mode 162

Security 171

Using the APC Security Wizard 190

Troubleshooting 205

How to Export Configuration Settings 208

APC Device IP Configuration Wizard 216

File Transfers 221

Product Information 232

Index 236

Introduction

Product Description

Features

The following APC Network Management Cards are web-based management products that use multiple, open standards such as Telnet, HTTP, HTTPS, SSL, TLS, SCP, and SNMP to provide full management of supported devices:

- AP9617 Network Management Card *EX*: The following is a list of some of this Management Card's features:
  - Provides the ability to export a user configuration (.ini) file from a configured card to one or more unconfigured cards without converting the file to a binary file
  - Generates system log (Syslog) messages
  - Allows using a Dynamic Host Configuration Protocol (DHCP) server to provide the Management Card's network (TCP/IP) values
  - Allows using the APC Remote Monitoring Service (RMS)
  - Provides data and event logs
  - Provides UPS scheduling features
  - Provides support for the APC PowerChute® Network Shutdown utility
  - Limits SNMP traps and e-mail notifications based on the severity level of the UPS or system events
  - Provides a selection of security protocols for authentication and encryption

- AP9618 Network Management Card *EM/MDM*: Includes all AP9617 features, and the following:
  - An Integrated Environmental Monitor that includes a temperature probe, input contacts, and an output relay.
  - An internal analog modem.
  - A paging feature that lets you configure any event so that a page will be sent to one or more configured analog or digital pagers when the event occurs. This feature includes call-back capabilities. An option lets you convert Network Management Card, UPS, and environmental monitoring event codes to the default Out-of-Band Management Card event codes (supplemented by several additional numerical codes).
- AP9619 Network Management Card *EM*: Includes all AP9617 features and an Integrated Environmental Monitor that includes a temperature probe, input contacts, and an output relay.

Note

Kits are available to upgrade AP9617 to include the features of AP9618 (AP9618U kit) or AP9619 (AP9619U kit). The AP9618U kit can also upgrade an AP9619 Management Card to include the AP9618 analog modem feature.

For an AP9618 Network Management Card *EM/MDM* or AP9619 Network Management Card *EM* you can also purchase a humidity probe from APC.

The Management Card can be installed into the following APC devices:

- Any Smart-UPS® or Matrix-UPS® model that has an internal expansion slot, as well as any Silcon™, Symmetra®, or Symmetra PX UPS

Note

A Silcon UPS, which does not have an expansion slot, requires using a Silcon Triple Expansion Chassis (AP9604S).

- Expansion Chassis (AP9600)
- Triple Expansion Chassis (AP9604)

Initial set-up

You must define three TCP/IP settings for the Network Management Card before it can operate on the network.

- IP address of the Management Card
- Subnet mask
- IP address of the default gateway

Note

Never use the loopback address (127.0.0.1) as the default gateway address for the Network Management Card. Doing so will disable the card and will require you to reset TCP/IP settings to their defaults using a local serial login.

See also

To configure the TCP/IP settings, see the Network Management Card *Installation and Quick Start Manual* provided in PDF (**.\doc\en\Insguide.pdf**) on the APC Network Management Card *utility* CD and in printed form.

To use a DHCP server to configure the TCP/IP settings at a Management Card, see Boot Mode.

Network management features

Following are some of the network management applications and utilities that can work with a UPS that connects to the network through a Network Management Card.

- APC network management applications:
  - PowerChute Network Shutdown provides unattended remote graceful shutdown of computers that are connected to APC UPSs.
  - APC InfraStruXure Manager provides enterprise-level power management and device management for APC agents, UPS models, information controllers, and environmental monitors.
  - PowerChute Business Edition provides departmental-level safe system shutdown and UPS management for workstations and servers.
  - APC InfraStruXure™ Manager provides the power management software for an InfraStruXure system.
- APC Wizard utilities
  - The APC Device IP Configuration Wizard configures the basic settings of one or more Network Management Cards over the network.
  - The APC Security Wizard creates components needed for high security for the Network Management Card on the network when you are using Secure Socket Layer (SSL) and related protocols and encryption routines.
- A Management Information Base (MIB) browser uses the OIDs of the APC MIB to perform SNMP SETs and GETs on a UPS.

Internal Management Features

Overview

The Management Card has two internal interfaces (control console and Web interface) which provide menus with options that allow you to manage the UPS, an environmental monitor (either the Integrated Environmental Monitor at an AP9618 or AP9619 Network Management Card or an external environmental monitor), and the Management Card. The Management Card's SNMP interface also allows you to use an SNMP browser with the PowerNet MIB to manage the UPS and environmental monitor.

For more information about the Management Card's internal user interfaces, see Control Console and Web Interface; for more information about how to use the APC MIB with an SNMP browser, see the *PowerNet® SNMP Management Information Base (MIB) Reference Guide* (**.\doc\en\Mibguide.pdf**), which is provided on the APC Network Management Card *utility* CD.

Access priority for logging on

Only one user at a time can log on to the Management Card to use its internal user interface features. The priority for access is as follows:

- Local access to the control console from a computer with a direct serial connection to the Management Card always has the highest priority.
- Telnet or Secure SHell (SSH) access to the control console from a remote computer has priority over Web access.
- Web access, either directly or through the InfraStruXure Manager, has the lowest priority.

📖 For information about how SNMP access to the Management Card is controlled, see SNMP.

Types of user accounts

The Management Card has three levels of access (Administrator, Device Manager, and Read-Only User), all of which are protected by user name and password requirements.

- An Administrator can use all of the management menus available in the control console and the Web interface. The Administrator's default **User Name** and **Password** values are both **apc**.
- A Device Manager can access only the **Log** option in the **Events** menu and use the UPS and **Environment** menus. The Device Manager's default user name is **device**, and the default password is **apc**.
- A Read-Only User has the following restricted access:
  - Access through the Web interface only.
  - Access to the same menus as a Device Manager, but without the capability to change configurations, control devices, delete data, or use FTP-related options. Links to configuration options are visible but disabled, and the event and data logs display no **Delete** button.

  The Read-Only User's default **User Name** is **readonly**, and the default **Password** is **apc**.

To set **User Name** and **Password** values for the three account types, see User Manager.

Note

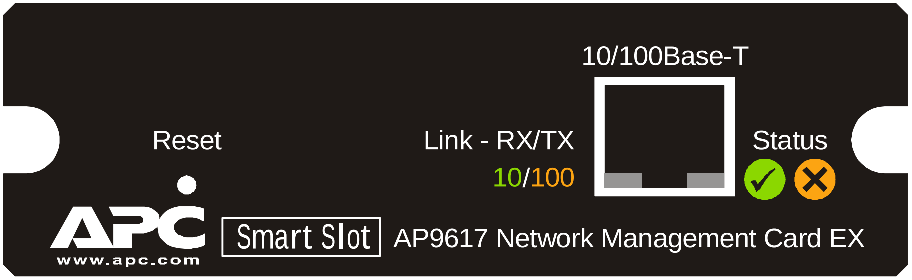
You must use the Web interface to configure values for the Read-Only User.

Front Panel

Introduction

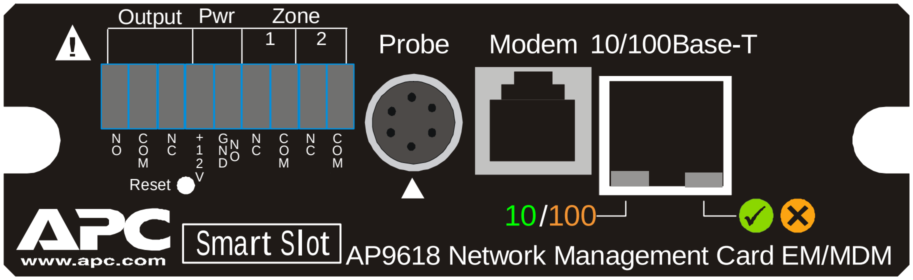
The figures below identify the front-panel features of the three versions (AP9617, AP9618, and AP9619) of the Network Management Card.

AP9617:



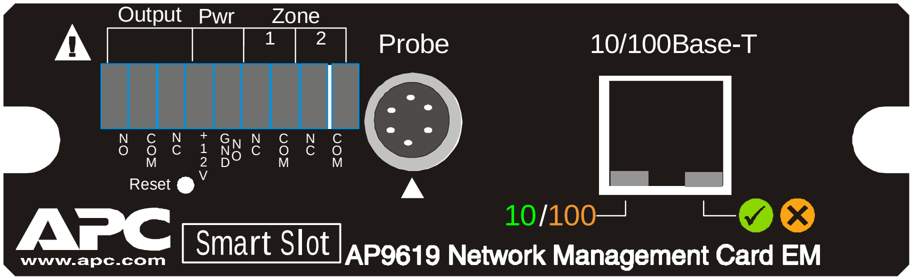
Includes Status LEDs, Reset button, and 10/100Base-T connector.

AP9618:



Includes the AP9617 features, an analog modem connector, and the Integrated Environmental Monitor's connections (for the probe, input contacts, and output relay).

AP9619:



Includes AP9617 features and the Integrated Environmental Monitor’s connections (for the probe, input contacts, and output relay).

Features

AP9618 or AP9619	**Description**
9-pin connector[1]	• Output relay (**Output**): Normally closed (**NC**), common (**COM**), and normally open (**NO**) pins used by the Integrated Environmental Monitor's output relay at an AP9618 or AP9619 Management Card. • Power (**Pwr**): Normally-open ground (**GND NO**) and **+12VDC** pins. • Input contacts (**Zone 1** and **2**): Two sets of normally closed (**NC**) and common (**COM**) pins used by the Integrated Environmental Monitor at an AP9618 or AP9619 Management Card.
Probe connector[1]	Connects a Temperature/Humidity probe to the Integrated Environmental Monitor at the AP9618 or AP9619 Management Card.
Modem connector[2] (AP9618 only)	Connects the internal analog modem at an AP9618 Management Card to an analog phone line to provide for out-of-band communications.
All Management Cards	**Description**
Reset button	Resets the Management Card while power remains on.
10/100 Base-T connector	Connects the Management Card to the Ethernet network.
Status LEDs	See Status LED.
Link-RX/TX (10/100) LED	See Link-RX/TX (10/100) LED.

[1] To manage the Integrated Environmental Monitor, see Environment Menu.

[2] To configure this feature for dial-in access to the control console at an AP9618 Network Management Card, see Modem (AP9618 control console).

Status LED

This LED indicates the Management Card's status.

Condition	Description
Off	One of the following situations exist: • The Management Card is not receiving input power • The Management Card is starting up. • The Management Card is not operating properly. It may need to be repaired or replaced. Contact APC Worldwide Customer Support.
Solid Green	The Management Card has valid TCP/IP settings.
Solid Orange	A hardware failure has been detected in the Management Card. Contact APC Worldwide Customer Support.
Flashing Green	The Management Card does not have valid TCP/IP settings.[1]
Flashing Orange	The Management Card is making BOOTP requests.[1]
Alternately flashing Green and Orange	If the LED is alternately flashing slowly, the Management Card is making DHCP[2] requests.[1] If the LED is alternately flashing rapidly, the Management Card is starting up.

[1] If you do not use a BOOTP or DHCP server, see the Network Management Card *Installation and Quick Start Manual* provided in printed format and on the APC Network Management Card *utility* CD in PDF (**.\doc\en\Insguide.pdf**) to configure the Management Card's TCP/IP settings.

[2] To use a DHCP server, see Boot Mode.

Link-RX/TX (10/100) LED

This LED indicates the network status.

Condition	**Description**
Off	One or more of the following situations exist: • The Management Card is not receiving input power. • The cable that connects the Management Card to the network is disconnected or defective. • The device that connects the Management Card to the network is turned off or not operating correctly. • The Management Card itself is not operating properly. It may need to be repaired or replaced. Contact APC Worldwide Customer Support.
Solid **Green**	The Management Card is connected to a network operating at 10 Megabits per second (Mbps).
Solid **Orange**	The Management Card is connected to a network operating at 100 Megabits per second (Mbps).
Flashing **Green**	The Management Card is receiving or transmitting data packets at 10 Megabits per second (Mbps).
Flashing **Orange**	The Management Card is receiving or transmitting data packets at 100 Megabits per second (Mbps).

Note

Using the 5-Port 10Base-T Hub SmartSlot Card eliminates the requirement for a separate hub power supply. However, this card requires that all Network Management Cards connected to it operate at 10 Mbps, not 100 Mbps.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the Management Card uses internal, system-wide watchdog mechanisms. When it restarts to recover from an internal problem, a **System: Warmstart** event is recorded in the event log.

Network interface watchdog mechanism

The Management Card implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the Management Card does not receive any network traffic for 9.5 minutes (either direct traffic, such as SNMP, or broadcast traffic, such as an Address Resolution Protocol [ARP] request), it assumes that there is a problem with its network interface and restarts.

Resetting the network timer

To ensure that the Management Card does not restart if the network is quiet for 9.5 minutes, the Management Card attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the Management Card, and that response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network most of the time and is on the same subnet. The network traffic of that computer will restart the 9.5-minute timer frequently enough to prevent the Management Card from restarting.

Control Console

How To Log On

Overview

You can use either a local (serial) connection, or a remote (Telnet or SSH) connection with a computer on the Management Card's subnet to access the control console. For an AP9618 Network Management Card, you can also use its internal analog modem to access the control console.

See Modem (AP9618 control console).

Use case-sensitive **User Name** and **Password** entries to log on (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device Manager). A Read-Only User has no access to the control console.

If you cannot remember your **User Name** or **Password**, see How to Recover from a Lost Password.

Remote access to the control console

You can access the control console through Telnet or Secure SHell (SSH), depending on which is enabled. (An Administrator can enable these access methods through the **Telnet/SSH** option of the **Network** menu.) By default, Telnet is enabled. Enabling SSH automatically disables Telnet.

Telnet for basic access. Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption. To use Telnet to access the control console from any computer on the same subnet:

1. At a command prompt, type `telnet` and the System IP address for the Management Card (when the Management Card uses the default Telnet port of 23), and press ENTER. For example:

```
telnet 139.225.6.133
```

Note: If the Management Card uses a non-default port number (between 5000 and 32767), you need to include a colon or a space (depending on your Telnet client) between the IP address and the port number.

2. Enter the user name and password (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device Manager).

SSH for high-security access. If you use the high security of SSL for the Web interface, use Secure SHell (SSH) for access to the control console. SSH encrypts user names, passwords and transmitted data.

The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

Local access to the control console

You can use a local computer, a computer that connects to the Management Card through the serial port at the Management Card's UPS or expansion chassis, to access the control console.

1. Select a serial port at the local computer and disable any service which uses that port.
2. Unless an APC smart-signaling cable (940-0024 or 940-1524) is already connected to the selected port, connect the smart-signaling cable that came with the Management Card to the selected port and to the serial port at the Management Card's UPS or chassis.
3. Run a terminal program (such as HyperTerminal®), and configure the selected port for 2400 bps, 8 data bits, no parity, 1 stop bit, and no flow control, and save the changes.
4. Press ENTER to display the **User Name** prompt.
5. Enter your user name and password.

How to Recover from a Lost Password

You can use a local computer, a computer that connects to the Management Card or other device through the serial port to access the control console.

1. Select a serial port at the local computer, and disable any service that uses that port.
2. Connect the serial cable (940-0024 or 940-1524) to the selected port on the computer and to the configuration port at the Management Card:
3. Run a terminal program (such as HyperTerminal®) and configure the selected port as follows:
   - 2400 bps
   - 8 data bits
   - no parity
   - 1 stop bit
   - no flow control.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   - The serial port is not in use by another application.
   - The terminal settings are correct as specified in step 3.
   - The correct cable is being used as specified in step 2.
5. Press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.
6. Press ENTER as many times as necessary to redisplay the **User Name** prompt, then use the default, **apc,** for the user name and password. (If

you take longer than 30 seconds to log on after the **User Name** prompt is redisplayed, you must repeat step 5 and log on again.)

7. From the **Control Console** menu, select **System**, then **User Manager**.
8. Select **Administrator**, and change the **User Name** and **Password** settings, both of which are now defined as **apc**.
9. Press CTRL-C, log off, reconnect any serial cable you disconnected, and restart any service you disabled.

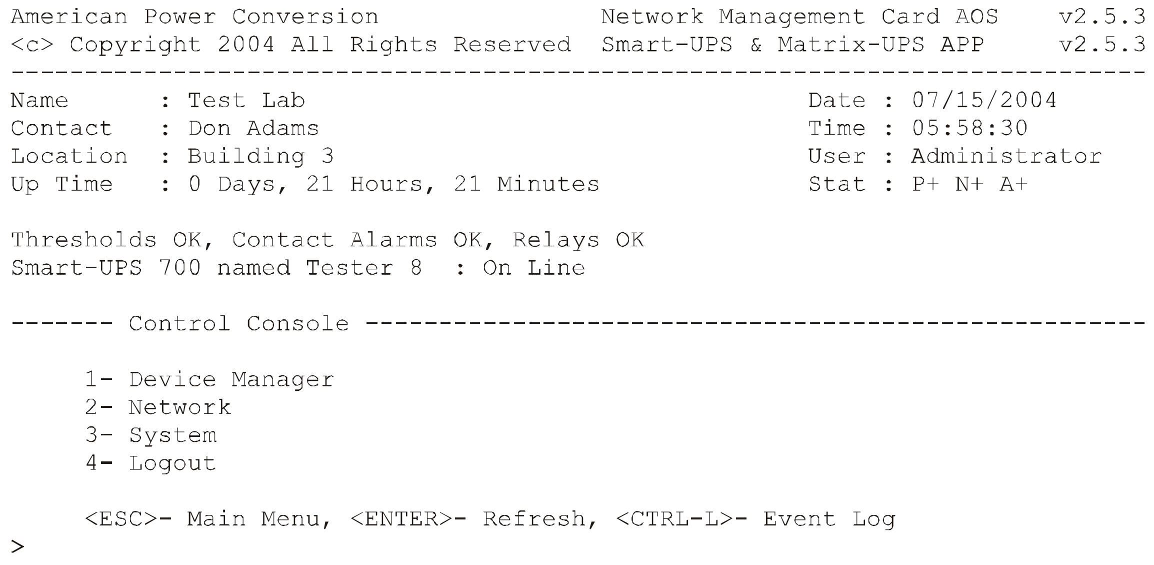
Main Screen

Example main screen

The following is an example of the screen that appears when you log on to the control console at an AP9618 or AP9619 Management Card that has the Integrated Environmental Monitor's output relay enabled. (An AP9617 does not have an Integrated Environmental Monitor, so it cannot report status for an output relay.)

Note

The **Relay OK** entry in the **Environment** status line indicates that the output relay is enabled and that no alarm condition exists.



```
American Power Conversion               Network Management Card AOS    v2.5.3
<c> Copyright 2004 All Rights Reserved  Smart-UPS & Matrix-UPS APP     v2.5.3
-----------------------------------------------------------------------------
Name      : Test Lab                                  Date : 07/15/2004
Contact   : Don Adams                                 Time : 05:58:30
Location  : Building 3                                User : Administrator
Up Time   : 0 Days, 21 Hours, 21 Minutes              Stat : P+ N+ A+

Thresholds OK, Contact Alarms OK, Relays OK
Smart-UPS 700 named Tester 8  : On Line

------- Control Console -----------------------------------------------------

     1- Device Manager
     2- Network
     3- System
     4- Logout

     <ESC>- Main Menu, <ENTER>- Refresh, <CTRL-L>- Event Log
>
```

Information and status fields

Main screen information fields.

- Two fields identify the APC operating system (AOS) and application (APP) firmware versions. The application firmware uses a name that identifies the type of UPS that the Management Card connects to the network. In the preceding example, the Management Card uses the application firmware for a UPS in the Smart-UPS/Matrix-UPS family, in this case, the Smart-UPS 700.

```
Network Management Card AOS   v2.5.3
Smart UPS & Matrix UPS APP    v2.5.3
```

- Three fields identify the system **Name**, **Contact**, and **Location** values.

```
Name       : Test Lab
Contact    : Don Adams
Location   : Building 3
```

For information about how to set the **Name**, **Contact**, and **Location** values, see System Menu.

- An **Up Time** field reports how long the Management Card has been running since it was last turned on or reset.

```
Up Time    : 0 Days 21 Hours 21 Minutes
```

- Two fields identify when you logged in, by **Date** and **Time**.

```
Date : 07/15/2004
Time : 5:58:30
```

- A **User** field identifies whether you logged in as **Administrator** or **Device Manager**. (The **Read Only User** account cannot access the Control Console.)

```
User : Administrator
```

Main screen status fields.

- A **Stat** field reports the Management Card status.

```
Stat : P+ N+ A+
```

`P+`	The APC operating system (AOS) is functioning properly.
`N+`	The network is functioning properly.
`N?`	A BOOTP request cycle is in progress.
`N–`	The Management Card failed to connect to the network.
`N!`	Another device is using the Management Card's IP address.
`A+`	The application is functioning properly.
`A–`	The application has a bad checksum.
`A?`	The application is initializing.
`A!`	The application is not compatible with the AOS.

Note

The AOS should always report that it is functioning properly (`P+`); If the AOS is not functioning properly, and you can not access the Management Card, see APC Worldwide Customer Support to contact APC support staff.

- A **UPS model and name** field reports the status of the UPS.

```
Smart-UPS 700 RM named Tester 8 : On Line
```

- The status of the probes (**Thresholds**) and contacts (**Contact Alarms**) at any environmental monitor, including the Integrated Environmental Monitor's output relay (**Relay**) at an AP9618 or AP9619 Management Card, is reported above the UPS status (**UPS model and name**) field.

```
Thresholds Ok, Contact Alarms Ok, Relay OK
```

For more information about the status of the UPS, see UPS Status; for more information about probe, contact, and output relay status, see Environment Menu.

Control Console Menus

Overview

The control console provides options to manage a Management Card, its UPS, and other supported devices. If a device is not present, the control console displays no options for that device. For example:

- The control console at a Management Card that connects with an environmental monitor only does not provide UPS options.
- The control console at an AP9618 or AP9619 Network Management Card displays options to manage its Integrated Environmental Monitor. These options are not available at the control console for an AP9617.

Main menu

The main **Control Console** menu has options that provide access to the control console's management features:

```
1- Device Manager
2- Network
3- System
4- Logout
```

Note

When you log on as Device Manager, you can access only the **Device Manager** menus and the **Logout** menu.

Menu structure

The menus in the control console list options by number and name. To use an option, type the option's number and press ENTER, then follow any on-screen instructions.

Options that allow you to change a setting have an **Accept Changes** option that you must use before you exit a menu to save the changes you made.

While in a menu, you can also do the following:

- Type ? and press ENTER, to access brief menu option descriptions (if the menu has help available)
- Press ENTER, to refresh the menu
- Press ESC, to go back to the menu from which you accessed the current menu
- Press CTRL-C, to return to the main (**Control Console**) menu
- Press CTRL-D, to toggle between the UPS and **Environment** menus
- Press CTRL-L, to access the event log

For information about the event log, see Event-Related Menus.

Device Manager option

This option accesses the **Device Manager** menu. This menu's options allow you to select the device that you want to manage:

```
1- Smart-UPS 700
2- Environment
```

The Environment option is displayed only when an environmental monitor is present. For an AP9618 or AP9619 Network Management Card, the Environment option accesses menu options use to configure the Integrated Environmental Monitor, as well as an external environmental monitor.

For information about the menu options that are available for managing a UPS, see UPS Menu; for information about the menu options that are available for managing environmental monitors, including the Integrated Environmental Monitor at an AP9618 or AP9619 Network Management Card, see Environment Menu.

Network option

To do any of the following tasks, see Network Menu:

- Configure the Management Card's TCP/IP settings, or, when the Management Card will obtain its TCP/IP settings from a server, configure the settings for the type of server (DHCP or BOOTP) to be used.
- Use the Ping utility.
- Define settings that affect the FTP, Telnet, Web interface and SSL, SNMP, e-mail, DNS, Syslog, and WAP (Wireless Application Protocol) features of the Management Card.
- Configure paging parameters for analog or Telolocator Alphanumeric Protocol (TAP) paging.

System option

To do any of the following tasks, see System Menu:

- Control **Administrator** and **Device Manager** access. (You can control **Read Only User** access by using the Web interface only.)
- Define the system **Name**, **Contact**, and **Location** values.
- Set the **Date** and **Time** used by the Management Card.
- Through the **Tools** menu:
  - Restart the Management Card.
  - Reset parameters to their default values.
  - Delete SSH host keys and SSL certificates.
- Configure modem parameters, including dial-in access to the control console at an AP9618 Network Management Card using that Management Card's internal analog modem.
- Access system information about the Management Card.

Web Interface

Introduction

Overview

The Web interface provides options that you use to manage a Management Card, its UPS, and other supported devices.

If a device is not present, the Web interface displays no options for that device. For example:

- The Web interface at a Management Card that connects with an environmental monitor only, will not provide UPS options.
- The Web interface at an AP9618 or AP9619 Network Management Card displays options to manage the Management Card's Integrated Environmental Monitor. These options are not available at the Web interface for an AP9617 Management Card, which has no Integrated Environmental Monitor.

📖 See Web/SSL for information on the menu options you use to select, enable, and disable the protocols that control access to the Web interface and to define the Web-server ports for the protocols.

Supported Web Browsers

As your browser, you can use Microsoft® Internet Explorer (IE) 5.0 (and higher) or Netscape® 4.0.8 (and higher, except Netscape 6.*x*) to access the Management Card through its Web interface. Other commonly available browsers also may work but have not been fully tested by APC.

Data verification, the event log, the data log, and Message Digest 5 (MD5) authentication require that you enable the following for your Web browser:

- JavaScript
- Java
- Cookies

In addition, the Management Card cannot work with a proxy server. Therefore, before you can use a Web browser to access its Web interface, you must do one of the following:

- Configure the Web browser to disable the use of a proxy server for the Management Card.
- Configure the proxy server so that it does not proxy the specific IP address of the Management Card.

How to Log On

Overview

You can use a Management Card's DNS name or System IP address for the URL address of the Web interface. Use your case-sensitive **User Name** and **Password** settings to log on. The default user name differs by account type:

- **apc** for an Administrator
- **device** for a Device Manager
- **readonly** for a Read-Only User

The default password is **apc** for all three account types.

Note

If you are using HTTPS (SSL/TSL) as your access protocol, your login credentials are compared with information in a server certificate. If the certificate was created with the APC Security Wizard, you must use an IP address to log on to the Management Card if an IP address was specified as the common name in the certificate, or you must use a DNS name to log on if a DNS name was specified as the common name in the certificate.

For information about the Web page that is displayed when you log on to the Web interface, see Summary Page.

URL address formats

Type the Management Card's DNS name or IP address in the Web browser's URL address field and press ENTER. Except when you specify a non-default web server port in Internet Explorer, `http://` or `https://` is automatically added by the browser.

Note

If the error "You are not authorized to view this page" occurs (Internet Explorer only), someone is logged onto the Web interface or control console. If the error "No Response" (Netscape) or "This page cannot be displayed" (Internet Explorer) occurs, Web access may be disabled, or the Management Card may use a non-default Web-server port that you did not specify correctly in the address. (For Internet Explorer, you must type `http://` or `https://`as part of the address when any port other than 80 is used.)

- For a DNS name of Web1, the entry would be one of the following:
  - `http://Web1` if HTTP is your access mode
  - `https://Web1` if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133, when the Management Card uses the default port (80) at the Web server, the entry would be one of the following:
  - `http://139.225.6.133` if HTTP is your access mode
  - `https://139.225.6.133` if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133, when the Management Card uses a non-default port (5000, in this example) at the Web server, the entry would be one of the following:
  - `http://139.225.6.133:5000` if HTTP is your access mode
  - `https://139.225.6.133:5000` if HTTPS (SSL/TLS is your access mode

Summary Page

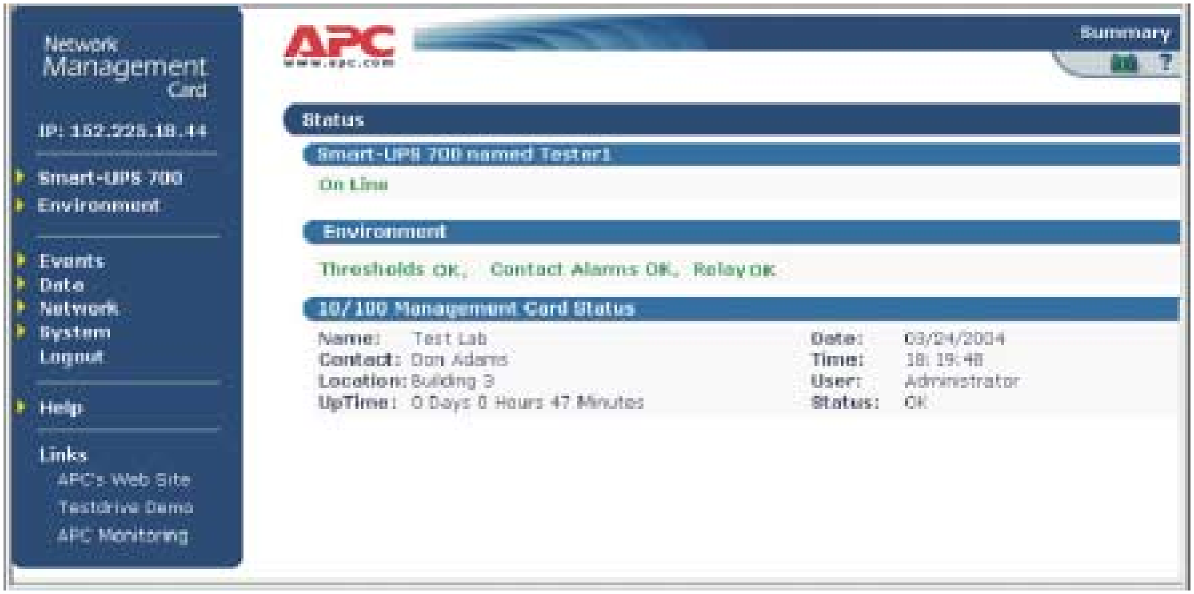
Example Web page

A navigation menu (see Navigation Menu) and “Summary” page are displayed when you log on to the Web interface. If you log on at an AP9618 or AP9619 Management Card, which has the Integrated Environmental Monitor, the summary page displays the status of the thresholds for the probe, the status of the input contacts, and the status of the output relay. (An AP9617 has no Integrated Environmental Monitor.)

See Settings Options to configure settings for the Integrated Environmental Monitor, including which event will activate the relay.

After the Management Card connects with a UPS, you can click the battery status icon on any Web interface page to access the “Summary Page.”

For more information about the help and status icons that can appear in the Web interface pages, see Quick status tab.



Status

Smart-UPS 700 named Tester1

On Line

Environment

Thresholds OK, Contact Alarms OK, Relay OK

10/100 Management Card Status

Name:	Test Lab	Date:	03/24/2004
Contact:	Don Adams	Time:	18:19:48
Location:	Building 3	User:	Administrator
UpTime:	0 Days 0 Hours 47 Minutes	Status:	OK

"Summary" page fields

The "Summary" page has three sections:

- The UPS section reports the status of a connected UPS. If the UPS is a Smart-UPS XLM model, the UPS section also reports, under **Outlet Group Status**, the name and status of each outlet group.
- The **Environment** section reports status for an environmental monitor, if either the Integrated Environmental Monitor of an AP9618 or AP9619 Network Management Card or an external environmental monitor is connected. Status of thresholds, input contacts, and output relay (if applicable) are displayed.
- The Management Card section reports the following information:
  - The **Name**, **Contact**, and **Location** information for the Management Card
  - The login date and time
  - Type of user (**Administrator**, **Device Manager**, or **Read Only User**)
  - How long (**Up Time**) the Management Card has been continuously running since it was turned on or reset
  - The status of the Management Card

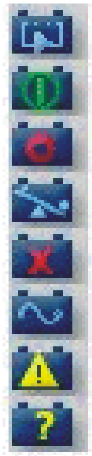
Quick status tab

Three types of icons can appear in the quick status tab in the upper-right corner of every Web interface page:

- A question mark (?) provides access to the online help for that page:

?

- When a UPS is connected, a battery icon identifies the current status of the UPS and accesses the “Summary” page from any other page:



The UPS is switched to bypass mode.

The UPS is operating normally.

The UPS is turned off.

The UPS is overloaded.

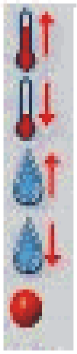
The UPS has a bad battery.

The UPS is switched to battery operation.

A fault exists at the UPS.

Communication with the UPS has been lost, or the UPS is unsupported.

- When an environmental monitor is connected, either an external environmental monitor or the Integrated Environmental Monitor at an AP9618 or AP9619, icons will identify any fault conditions:



A high-temperature threshold violation exists.

A low-temperature threshold violation exists.

A high-humidity threshold violation exists.

A low-humidity threshold violation exists.

States which contact device has a fault: either an input contact or the output relay at an AP9618 or AP9619 Management Card's Integrated Environmental Monitor.

Navigation Menu

Overview

When you log on to the Web interface as an Administrator, the navigation menu (left frame) contains the following elements:

- The Management Card's IP address
- A UPS menu which uses the UPS model for its name (**Smart-UPS 700**, in the example on Example Web page)
- An **Environment** menu (if an environmental monitor is discovered)
- An **Events** menu
- A **Data** menu
- A **Network** menu
- A **System** menu

Note

When you log on as a Device Manager or Read-Only User, the **Network** and **System** menus do not appear in the navigation menu. Options to make any changes are not available for the Read-Only User.

- A **Logout** option
- A **Help** menu
- A **Links** menu

Selecting a menu to perform a task

Use the menus to perform tasks as follows:

- To manage a UPS, and to set up and manage Synchronized Control Groups of Smart-UPS or Symmetra UPSs, see UPS Menu.
- To manage an environmental monitor, including the AP9618 or AP9619 Network Management Card's Integrated Environmental Monitor, see Environment Menu.
- To do the following, see Event-Related Menus:
  - Access the Event Log.
  - Configure the actions to be taken based on an event's severity level.
  - Configure SNMP Trap Receiver settings to send event-based traps.
  - Define who will receive e-mail notifications of events.
- To do the following, see Data Menu (Web Interface Only):
  - Access the Data Log.
  - Define the log interval (how often data will be sampled and recorded) for the Data Log.
- To do the following, see Network Menu:
  - Configure new TCP/IP settings for the Management Card.
  - Identify the Domain Name Service (DNS) Server, test its network connection, and enable or disable DNS Reverse Lookup Event Logging (which logs the domain name of the device associated with each event).
  - Define settings for FTP, Telnet, SSH, the Web interface, SNMP, e-mail, and SSL/TLS.
  - Configure the Management Card's Syslog message feature.
  - For Management Cards associated with UPS models in the Smart-UPS product line only, enable or disable access to the Management Card by users of the Wireless Application Protocol (WAP).
  - Configure paging parameters for analog or Telolocator Alphanumeric Protocol (TAP) paging.

- To do the following, see System Menu.
  - Control **Administrator**, **Device Manager**, and **Read Only User** access.
  - Define the system **Name**, **Contact**, and **Location** values.
  - Set the **Date** and **Time** values used by the Management Card.
  - Through the **Tools** menu:
    - Restart the Management Card.
    - Reset parameters to their default values.
    - Delete SSH host keys and SSL certificates
    - Upload an initialization file (.ini file) that has been downloaded from another Management Card. The current Management Card then uses the values in that .ini file to configure its own settings.
  - Select **Fahrenheit** or **Celsius** for temperature displays.
  - Define the URL addresses used by the Web interface's user and APC logo links, as described in Links menu.

Help menu

When you click **Help**, the **Contents** page for the online help is displayed to provide for easy navigation to a specific online help topic. However, from any of the Web interface pages, you can use the question mark (**?**) that appears in the quick status bar to link to the section of the online help for that page's content.

Use the **Help** menu's **About System** option to view information about the Management Card's **Model Number**, **Serial Number**, **Hardware Revision**, **Manufacture Date**, **MAC Address, Application Module** and **APC OS (AOS) Module**, including the date and time these modules were created.

See also

For help on the type of flash memory used, see **Flash Type** in the **About System** option of the control console's **System** menu.

Links menu

This menu provides three user-definable URL link options. By default, these links access the following APC web pages:

- **APC's Web Site** accesses the APC home page.
- **Testdrive Demo** accesses a demonstration page where you can use samples of APC web-enabled products.
- **APC Monitoring** accesses the "APC Remote Monitoring Service" page where you can find more information about monitoring services available from APC at an additional cost.

You can use the following procedure to redefine these links so that they point to other URLs, such as those of other UPS devices, MasterSwitch devices, and servers that are being powered by the UPS.

1. Click on **Links** in the **System** menu.
2. Define any new names for the **User Links**.
3. Define any new valid URL addresses that you want the **User Links** to access.
4. Click **Apply**.

Network Menu

Introduction

Overview

The **Network** menu has the options that you use to do the following tasks:

- Define TCP/IP settings, including DHCP or BOOTP server settings, when one of those types of servers is used to provide the required TCP/IP values
- Use the Ping utility
- Define and display settings that affect the Management Card's settings for DNS, FTP, Telnet, SSH, SNMP, E-mail, Syslog, the Web interface (SSL/TLS), and WAP (for Smart-UPS models only).
- Set up and configure the paging features available if you have an AP9618 Network Management Card *EM/MDM*, which has an internal analog modem.

Note

Only an Administrator has access to the **Network** menu.

Menu options

Unless noted, the following menu options are available in the control console and Web interface:

- TCP/IP
- DNS
- Send DNS Query (Web interface)
- Ping utility (control console)
- FTP Server
- Telnet/SSH
- SNMP
- Email
- Syslog
- Web/SSL
- WAP (for Smart-UPS models only)
- Paging

Option Settings

TCP/IP

This option accesses the following settings:

- A Boot mode setting selects the method used to define the TCP/IP values that a Management Card needs to operate on the network:
  - **System IP**: The IP address of the Management Card
  - **Subnet Mask**: The subnet mask value
  - **Default Gateway**: The IP address of the default gateway

  For information about the watchdog role of the default gateway, see Resetting the network timer. To configure the initial TCP/IP settings when you install the Management Card, see the Network Management Card *Installation and Quick Start Manual* **(.\doc\en\insguide.pdf**), provided on the APC Network Management Card *utility* CD and in printed form.

- Advanced settings define the Management Card's host and domain names, as well as Ethernet port speed, BOOTP, and DHCP settings used by the Management Card.

Current TCP/IP settings fields. The current values for **System IP**, **Subnet Mask**, and **Default Gateway**, and the Management Card's **MAC Address**, **Host Name**, **Domain Name**, and **Ethernet Port Speed** values are displayed above the TCP/IP settings in the control console and the Web interface.

Boot mode setting. This setting selects which method will be used to define the Management Card's TCP/IP settings whenever the Management Card turns on, resets, or restarts:

- **Manual**: Three settings (**System IP**, **Subnet Mask**, and **Default Gateway**) which are available only when **Manual** is used to define the needed TCP/IP settings.
- **BOOTP only**: A BOOTP server provides the TCP/IP settings.
- **DHCP only**: A DHCP server provides the TCP/IP settings.
- **DHCP & BOOTP**: The Management Card will attempt to get its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server.

Note

An **After IP Assignment** setting, by default, will switch **Boot mode** from its default **DHCP & BOOTP** setting to **BOOTP only** or **DHCP only**, depending on the type of server that supplied the TCP/IP settings to the Management Card.

For information about the **After IP Assignment** setting, and other settings that affect how the Management Card uses BOOTP and DHCP, see Advanced settings; For more information about how to use DHCP, see Boot Mode.

Advanced settings. The boot mode affects which settings are available:

- Two settings are available for all **Boot mode** selections to define the Management Card's **Host Name** and **Domain Name** values.
  - **Host Name:** When an Administrator configures a host name here and a domain name in the **Domain Name** field, users can then enter a host name in any field in the Network Management Card interface (except e-mail addresses) that accepts a domain name as input.
  - **Domain Name**: An Administrator needs to configures the domain name here only. In all other fields in the Network Management Card interface (except e-mail addresses) that accept domain names, the Management Card will add this domain name when only a host name is entered.

  Note

  To override the expansion of a specified host name by the addition of the domain name, do one of the following:

  - To override the behavior in all instances, set the domain name field in **Configure General Settings** to its default `somedomain.com` or to `0.0.0.0`.
  - To override the behavior for a particular host name entry — for example when defining a trap receiver — include a trailing period. The Network Management Card recognizes a host name with a trailing period (such as *`mySnmpServer.`*) as if it were a fully qualified domain name and therefore does not append the domain name.
- A **Port Speed** setting is available for all **Boot mode** selections to define the TCP/IP port's communication speed (**Auto-negotiate**, by default).
- Three settings are available for all **Boot mode** selections, except **Manual**, to identify the Management Card in BOOTP or DHCP communication:

- **Vendor Class**: Uses **APC**, by default.
- **Client ID**: Uses the Management Card's MAC address, by default.

Caution **IF THE CLIENT ID IS CHANGED FROM THE MANAGEMENT CARD'S MAC ADDRESS, THE NEW VALUE MUST BE UNIQUE ON THE LAN. OTHERWISE, THE DHCP OR BOOTP SERVER MAY ACT INCORRECTLY.**

- **User Class**: Uses the Management Card's application firmware module type, by default. For example, a Symmetra module sets the **User Class** to **SY**, and a Smart-UPS/Matrix-UPS module sets it to **SUMX**.

- Two settings are available if **BOOTP only** is the Boot mode selection:
  - **Retry Then Fail**: Defines how many times the Management Card will attempt to discover a BOOTP server before it stops (4, by default).
  - **On Retry Failure**: Defines what TCP/IP settings will be used by the Management Card when it fails to discover a BOOTP server (**Use Prior Settings**, by default).

For information about the **Advanced** settings (**DHCP Cookie Is** and **Retry Then Stop**) that directly affect how DHCP is used, see Boot Mode.

DNS

Use this option to define the IP addresses of the primary and secondary Domain Name Servers (DNS) used by the Management Card's e-mail feature. The primary DNS server will always be tried first.

See E-mail Feature and DNS servers.

Send DNS Query (Web interface). Use this option, available only through the **DNS** menu in the Web interface, to send a DNS query that tests the setup of your DNS servers.

Use the following settings to define the parameters for the test DNS request; you view the result of the test DNS request in the **Last Query Response** field (which displays **No last query** or text describing the query result of the last test).

- Use the **Query Type** setting to select the method to use for the DNS query:
  - The URL name of the server (**Host**)
  - The IP address of the server (**IP**)
  - The fully qualified domain name (**FQDN**)
  - The Mail Exchange used by the server (**MX**)
- Use the **Query Question** text field to identify the value to be used for the selected **Query Type**:
  - For **Host**, identify the URL
  - For **IP**, identify the IP address
  - For **FQDN**, identify the fully qualified domain name, formatted as `myserver.mydomain.com`.
  - For **MX**, identify the Mail Exchange address
- Enable or disable **Reverse DNS Lookup**, which is disabled by default. Enable this feature unless you have no DNS server configured or have poor network performance because of heavy network traffic. With **Reverse DNS Lookup** enabled, when a network-related event occurs, reverse DNS lookup logs in the event log both the IP address and the domain name for the networked device associated with the event. If no domain name entry exists for the device, only its IP address is logged with the event. Since domain names generally change much less frequently than IP addresses, enabling reverse DNS lookup can improve the ability to identify addresses of networked devices that are causing events to occur.

Ping utility (control console)

Select this option, available only in the control console, to check the Management Card's network connection by testing whether a defined IP address or domain name responds to the Ping network utility. By default, the default gateway IP address (see TCP/IP) is used. However, you can use the IP address or domain name of any device known to be running on the network.

FTP Server

Use the **Access** setting to enable or disable the FTP server. The server is enabled by default.

Note

FTP transfers files without using encryption. For higher security, use Secure CoPy (SCP) for file transfers. When you select and configure Secure SHell (SSH), SCP is enabled automatically. If you decide to use SCP for file transfer, be sure to disable the FTP server.

To configure SSH, see Telnet/SSH

Use the **Port** setting to identify the TCP/IP port that the FTP server uses for communications with the Management Card. The default **Port** setting is **21**.

You can change the **Port** setting to any unused port from **5000** to **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port. For example, for a port number of 5000 and a Management Card IP address of 152.214.12.114, you would use this command:

```
ftp 152.214.12.114:5000
```

To access a text version of the Management Card's event or data log, see How to use FTP or SCP to retrieve log files.

To use FTP to download configuration files:

- See File Transfer (control console only) if the files are on an FTP server of your company or agency.
- See Firmware file transfer methods if you are downloading files from the APC Web site.

Telnet/SSH

Use the **Telnet/SSH** option to perform the following tasks:

- Enable or disable Telnet or the Secure SHell (SSH) protocol for remote control console access.
  - While SSH is enabled, you cannot use Telnet to access the control console.
  - Enabling SSH enables SCP automatically.

    Note When SSH is enabled and its port and encryption ciphers configured, no further configuration is required to use SCP. (SCP uses the same configuration as SSH.)

  - Do not enable both versions of SSH unless you require that both be activated at the same time. (Security protocols use extensive processing power.)

  Note To use SSH, you must have an SSH client installed. Most Linux and other UNIX® platforms include an SSH client as part of their installation, but Microsoft Windows operating systems do not. SSH clients are available from various vendors.

- Configure the port settings for Telnet and SSH.
- Select one or more data encryption algorithms for SSH version 1, SSH version 2, or both.
- In the Web interface, specify a host key file previously created with the APC Security Wizard and load it to the Management Card.

Note

From a command line interface, such as the command prompt on Windows operating systems, you can use FTP or Secure CoPy (SCP) to transfer the host key file. You must transfer the file to location **/sec** on the Management Card.

If you do not specify a host key file, the Network Management Card generates an RSA host key of 768 bits, instead of the 1024-bit RSA host key that the Wizard creates. **The Management Card can take up to 5 minutes to create this host key, and SSH is not accessible during that time.**

- Display the *fingerprint* of the SSH host key for SSH versions 1 and 2. Most SSH clients display the fingerprint at the start of a session. Compare the fingerprint displayed by the client to the fingerprint that you recorded from the Web interface or control console of the Management Card.

Note

If you are using SSH version 2, expect a noticeable delay when logging on to the control console of the Management Card. Although the delay is not long, it can be mistaken for a problem because there is no explanatory message.

Option	Description
Telnet/SSH Network Configuration	
Access	Enables or disables the access method selected in **Protocol Mode**. **NOTE:** Enabling SSH automatically disables Telnet. To enable SSH, change the setting and then click **Next>>** in the Web interface or choose **Accept Changes** in the control console. You must then agree to the license agreement that is displayed
Protocol Mode	Choose one of the following: • **Telnet:** User names, passwords, and data are transmitted without encryption. • **Secure SHell (SSH) version 1:** User names, passwords and data are transmitted in encrypted form. There is little or no delay when you are logging on. • **Secure SHell (SSH) version 2:** User names, passwords and data are transmitted in encrypted form, but with somewhat more protection than version 1 from attempts to intercept, forge, or alter data during data transmission. There is a noticeable delay when you are logging on to the Management Card. • **Secure SHell (SSH) versions 1 and 2**: Do not enable both versions of SSH unless you require that both be activated at the same time. (Security protocols use extensive processing power.)

Option	Description
Telnet/SSH Port Configuration	

Telnet Port	Identifies the TCP/IP port used for communications by Telnet with the Management Card. The default is **23**.
	You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. Then, according to the requirements of your Telnet client program, you must use either a colon (:) or a space in the command line to specify the non-default port number. For example, for a port number of 5000 and a Management Card IP address of 152.214.12.114, your Telnet client would require one or the other of the following commands:
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`

SSH Port	Identifies the TCP/IP port used for communications by the Secure SHell (SSH) protocol with the Management Card. The default is **22**. You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. See the documentation for your SSH client for information on the command line format required to specify a non-default port number when starting SSH.

Option	Description
SSH Server Configuration	
SSHv1 Encryption Algorithms	Enables or disables **DES**, and displays the status (always enabled) of **Blowfish**, two encryption algorithms (block ciphers) compatible with SSH version 1 clients. • **DES**: The key length is 56 bits. • **Blowfish**: The key length is 128 bits. You cannot disable this algorithm. **NOTE:** Not all SSH clients can use every algorithm. If your SSH client cannot use **Blowfish**, you must also enable **DES**.
SSHv2 Encryption Algorithms	Enables or disables the following encryption algorithms (Block Ciphers) that are compatible with SSH version 2 clients. • **3DES** (enabled by default): The key length is 168 bits. • **Blowfish** (enabled by default): The key length is 128 bits. • **AES 128**: The key length is 128 bits. • **AES 256**: The key length is 256 bits. **NOTE:** Not all SSH clients can use every algorithm. Your SSH client selects the algorithm that provides the highest security from among the enabled algorithms that it is able to use. (If your SSH client cannot use either of the default algorithms, you must enable an AES algorithm that it can use.)

Option	Description
SSH User Host Key File	
Status:	The **Status** field Indicates the status of the host key (*private* key). In the control console, you display host key status by selecting **Advanced SSH Configuration**. • **SSH Disabled: No host key in use**: SSH currently is disabled and is not using a host key. A host key may or may not be loaded. **NOTE:**A host key must be installed to the **/sec** directory of the Management Card • **Generating**: The Management Card is generating a host key because no valid host key was installed in its **/sec** directory. • **Loading**: A host key is being loaded (i.e., being activated on the Management Card). • **Valid**: The host key is valid. (If you install an invalid host key, the Management Card discards it and generates a valid one. However, a host key that the Management Card generates is only 768 bits in length. A valid host key created by the APC Security Wizard is 1024 bits.)
Filename:	You can create a host key file with the APC Security Wizard and then upload it to the Management Card by using the Web interface. Use the **Browse** button for the **Filename** field to locate the file, then click **Apply**. Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the host key file to the Management Card. **NOTE:** Creating and uploading a host key in advance reduces the time required to enable SSH. If no host key is loaded when you enable SSH, the Management Card creates one when it reboots. **The Management Card takes up to 5 minutes to create this key, and the SSH server is not accessible during that time.**

Option	Description
SSH Host Key Fingerprint	
SSH v1:	Displays the SSH version 1 fingerprint for the host key. The fingerprint is a unique identifier to further authenticate the host key. In the control console, choose **Advanced SSH Configuration** and then **Host Key Information** to display the fingerprint.
SSH v2:	Displays the SSH version 2 fingerprint for the host key. The fingerprint is a unique identifier to further authenticate the host key. In the control console, choose **Advanced SSH Configuration** and then **Host Key Information** to display the fingerprint.

SNMP

An **Access** option (**Settings** in the control console) enables (by default) or disables SNMP. When SNMP is enabled, the **Access Control** settings allow you to control how each of the four available SNMP channels is used.

To define up to four NMSs as trap receivers, see Trap Receivers; to use SNMP to manage a UPS or an environmental monitor, see the *PowerNet*® *SNMP Management Information Base (MIB) Reference Guide* (**.\doc\en\mibguide.pdf**) on the APC Network Management Card *utility* CD.

Setting	**Definition**
Community Name	This setting defines the password (maximum of 15 characters) which an NMS that is defined by the **NMS IP** setting uses to access the channel.
NMS IP/ Domain Name	Limits access to the NMS specified by a domain name or to the NMSs specified by the format used for the IP address: • A domain name allows only the NMS at that location to have access. • 159.215.12.1 allows only the NMS with that IP address to have access. • 159.215.12.255 allows access for any NMS on the 159.215.12 segment. • 159.215.255.255 allows access for any NMS on the 159.215 segment. • 159.255.255.255 allows access for any NMS on the 159 segment. • 0.0.0.0 or 255.255.255.255 allows access for any NMS.

Setting	Definition	
Access Type	Selects how the NMS defined by the NMS IP setting can use the channel, when that NMS uses the correct **Community Name**.	
	Read	The NMS can use GETs at any time, but it can never use SETs.
	Write	The NMS can use GETs at any time, and can use SETs when no one is logged on to the control console or Web interface.
	Disabled	The NMS cannot use GETs or SETs.
	Write+	The NMS can use GETs and SETs at any time, even when someone is logged on to the control console or Web interface.

Email

You use this option to define two SMTP settings (**SMTP Server** and **From Address**) used by the Management Card's e-mail feature.

See SMTP settings and E-mail Feature.

Syslog

By default, the Management Card can send messages to up to four Syslog servers whenever Management Card, environmental monitor, or UPS events occur. The Syslog servers, which must be specifically identified by their IP addresses or domain names, record the events in a log that provides a centralized record of events that occur at network devices.

See also

This user's guide does not describe Syslog or its configuration values in detail. For more information about Syslog, see RFC3164, at **www.ietf.org/rfc/rfc3164**.

Syslog settings. Leave the Syslog settings, except the **Server IP** settings, set to their defaults unless otherwise specified by the Syslog network or system administrator.

Setting	Definition
General Settings	
Syslog	Enables (by default) or disables the Syslog feature.
Facility	Selects the facility code assigned to the Management Card's Syslog messages (**User**, by default). **NOTE:** Although several daemon-specific and process-specific selections are available, along with eight generic selections, **User** is the selection that best defines the Syslog messages sent by a Management Card.
Syslog Server Settings	
Server IP/ Domain Name	Uses specific IP addresses or domain names to Identify which of up to four servers will receive Syslog messages sent by the Management Card. **NOTE:** To use the Syslog feature, at least **Server IP/Domain Name** must be defined for at least one server.
Port	Identifies the user datagram protocol (UDP) port that the Management Card will use to send Syslog messages. The default is **514**, the number of the UDP port assigned to Syslog.

Setting	Definition
Local Priority (Severity Mapping)	
Map to Syslog's Priorities	Maps each of the severity levels (**Local Priority** settings) that can be assigned to UPS, environmental monitor, and Management Card events to the available Syslog priorities. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the four **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** • **None** (for events that have no severity level assigned) is mapped to **Info** **NOTE:** To disable sending Syslog messages for **Severe**, **Warning**, or **Informational** events, see Event Actions (Web Interface Only).

Syslog test (Web interface). This option allows you to send a test message to the Syslog servers configured in the **Syslog Server** section.

1. Select the priority you want to assign to the test message.
2. Define the test message, using any text that is formatted as described in Syslog message format below. For example, `APC: Test message`, meets the required message format.
3. Click **Apply** to have the Management Card send a Syslog message that uses the defined **Priority** and **Test Message** settings.

Syslog message format. A Syslog message has three parts:

- The priority (PRI) part identifies the Syslog priority assigned to the message's event and the facility code assigned to messages sent by the Management Card.
- The Header includes a time stamp and the IP address of the Management Card.
- The message (MSG) part has two fields:
  - A TAG field, which is followed by a colon and a space, identifies the event type (APC, System, or UPS, for example)
  - A CONTENT field provides the event text, followed by a space and the event code

Web/SSL

Use the **Web/SSL** menu to perform the following tasks.

- Enable or disable the two protocols that provide access to the Web interface of the Network Management Card:
  - Hypertext Transfer Protocol (HTTP) provides access by user name and password, but does not encrypt user names, passwords, and data during transmission.
  - Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). Secure Socket Layer (SSL) encrypts user names, passwords, and data during transmission and provides authentication of the Network Management Card by means of digital certificates.

    See Creating and Installing Digital Certificates to choose among the several methods for using digital certificates.
- Configure the ports that each of the two protocols will use.
- Select the encryption ciphers that SSL will use.
- Identify whether a server certificate is installed on the Management Card. If a certificate has been created with the APC Security Wizard but is not installed:
  - In the Web interface, browse to the certificate file and upload it to the Management Card.
  - Alternatively, use the Secure CoPy (SCP) protocol or FTP to upload it to the location **\sec** on the Management Card

Note

Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL/TLS). If no server certificate is loaded when you enable HTTPS (SSL/TLS), the Management Card creates one when it reboots. **The Management Card can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.**

- Display the configured parameters of a digital server certificate, if one is installed.

Option	**Description**
Web/SSL Network Configuration	
Access	Enables or disables the access method selected in **Protocol Mode**.
Protocol Mode	Choose one of the following: • **HTTP:** User names, passwords, and data are transmitted without encryption. • **HTTPS (SSL/TLS):** User names, passwords and data are transmitted in encrypted form, and digital certificates are used for authentication. **NOTE:** To enable HTTPS (SSL/TLS), change the setting and then click **Next>>** in the Web interface, or choose **Accept Changes** in the control console. You must then agree to the license agreement that is displayed. To activate the changes you must log off and log back on to the interface. When SSL is activated, your browser displays a lock icon, usually at the bottom of the screen.

Option	Description
HTTP/HTTPS Port Configuration	
HTTP Port	Identifies the TCP/IP port used for communications by HTTP with the Management Card. The default is **80**. You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 5000 and a Management Card IP address of 152.214.12.114, you would use this command: `http://152.214.12.114:5000`
HTTPS Port	Identifies the TCP/IP port used for communications by HTTPS with the Management Card. The default is **443**. You can change the **Port** setting to the number of any unused port between **5000** and **32768** to enhance the protection provided by **User Name** and **Password** settings. You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 6502 and a Management Card IP address of 152.214.12.114, you would use this command: `https://152.214.12.114:6502`

Option	Description
SSL Server Configuration	
CipherSuite	Enables or disables the following SSL encryption ciphers and hash algorithms. (To access these options in the control console, choose **Web/SSL**, then **Advanced SSL/TLS Configuration**.) **NOTE:** All of these encryption ciphers and hash algorithms use the RSA public key algorithm. • **DES (SSL_RSA_WITH_DES_CBC_SHA)**: a block cipher with a key length of 56 bits. The Secure Hash Algorithm (SHA) is used for authentication. • **3DES (SSL_RSA_WITH_3DES_EDE_CBC_SHA)**: a block cipher with a key length of 168 bits. A Secure Hash Algorithm (SHA) is used for authentication. • **RC4 (SSL_RSA_WITH_RC4_128_MD5)**: a stream cipher with a key length of 128 bits, with an RSA key exchange algorithm, and with a Message Digest 5 (MD5) hash algorithm used for authentication. This selection is enabled by default. • **RC4 (SSL_RSA_WITH_RC4_128_SHA)**: a stream cipher with a key length of 128 bits. A Secure Hash Algorithm (SHA) is used for authentication. This selection is enabled by default.

Option	Description
SSL/TLS Server Certificate	
Status:	The **Status** field indicates whether a server certificate is installed. (To display the status in the control console, choose **Web/SSL/TLS**, then **Advanced SSL/TLS Configuration**.) • **Not installed**: No certificate is installed on the Management Card. **NOTE:**If you install a certificate by using FTP or SCP, you must specify the correct location (**/sec**) on the Management Card. • **Generating**: The Management Card is generating a certificate because no valid certificate was installed. • **Loading**: A certificate is being loaded (activated on the Management Card). • **Valid**: A valid certificate was installed to or generated by the Management Card. (If you install an invalid certificate, the Management Card discards it and generates a valid one. However, a certificate that the Management Card generates has some limitations. See Method 1: Use the Network Management Card's auto-generated default certificate.)
Filename:	You can create a server certificate with the APC Security Wizard and then upload it to the Management Card by using the Web interface. Use the **Browse** button for the **Filename** field to locate the file, then click **Apply**. By default, the certificate is installed to the correct location. Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Management Card. However, you must specify the correct location (**/sec**) on the Management Card. **NOTE:** Creating and uploading a server certificate in advance reduces the time required to enable HTTPS (SSL/TLS). If no server certificate is loaded when you enable HTTPS (SSL/TLS), the Management Card creates one when it reboots. **The Management Card can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time**.

Parameter	**Description**
Current Certificate Details	
Issued to:	**Common Name (CN)**: The IP Address or DNS name of the Management Card, except if the server certificate was generated by default by the Management Card. For a default server certificate, the **Common Name (CN)** field displays the Management Card's serial number. **NOTE:** If an IP address was specified as the Common Name when the certificate was created, use an IP address to log on to the Web interface of the Management Card; if the DNS name was specified as the Common Name, use the DNS name to log on. When you log on, if you do not use the IP address or DNS name that was specified for the certificate, authentication fails, and you receive an error message asking if you want to continue. **Organization (O)**, **Organizational Unit (OU)**, and **Locality, Country:** The name, organizational unit, and location of the organization that is using the server certificate. If the server certificate was generated by default by the Management Card, the **Organizational Unit (OU)** field displays "Internally Generated Certificate." **Serial Number**: The serial number of the server certificate.
Issued By:	**Common Name (CN)**: The Common Name as specified in the CA root certificate, except if the server certificate was generated by default by the Management Card. For a default server certificate, the **Common Name (CN)** field displays the Management Card's serial number. **Organization (O)** and **Organizational Unit (OU)**: The name and organizational unit of the organization that issued the server certificate. If the server certificate was generated by default by the Management Card, the **Organizational Unit (OU)** field displays "Internally Generated Certificate."
Validity	**Issued on**: The date and time at which the certificate was issued. **Expires on**: The date and time at which the certificate expires.

Parameter	Description
Fingerprints	Each of the two fingerprints is a long string of alphanumeric characters punctuated by colons. A fingerprint is a unique identifier that you can use to further authenticate the server. Record the fingerprints to compare with the fingerprints contained in the certificate, as displayed in the browser. **SHA1 Fingerprint**: This fingerprint is created by a Secure Hash Algorithm (SHA). **MD5 Fingerprint**: This fingerprint is created by a Message Digest 5 (MD5) algorithm.

WAP (for Smart-UPS models only)

Use this option to enable (the default) or disable the *Wireless Application Protocol (WAP)*. WAP is a standard for providing cellular phones, pagers and other handheld devices with secure access to e-mail and text-based Web pages. WAP runs on all major wireless networks and is device-independent, so that it can be used with many phones and handheld devices.

Paging

Use this option to display and configure information about paging recipients and *Telolocator Alphanumeric Protocol (TAP)* carriers, and to set up and test paging. TAP is the most common digital paging protocol.

Note

This paging feature requires an AP9618 Network Management Card *EM/MDM*. An AP9618U kit is available to upgrade an AP9617 Network Management Card *EX* or an AP9619 Network Management Card *EM* to include the features of AP9618.

Configure TAP Carriers. If any of your paging recipients will use *Telolocator Alphanumeric Protocol (TAP)*, configure their TAP carriers (service providers). You can configure the required information for up to four TAP carriers through the **Paging** option of the **Network** menu.

TAP Carrier Parameter	Description
Carrier Name	The name of the TAP carrier (service provider). When you configure paging recipients later, you can designate a carrier for each recipient from among the names of configured carriers.
Phone Number	The telephone number of the gateway of the TAP carrier: • Include, at the start of this phone number, any numerals you must dial to access an external telephone line — for example, 9. • Include a comma to cause the modem to pause to wait for a dial tone. • End the dial string with the telephone number of the TAP gateway, as provided to you by the TAP carrier. **Example:** 9,15556789000
Parity	The parity required for a connection by modem to a TAP paging terminal of this TAP carrier. Choose `Even`, `Odd`, or `None`, according to the information provided by the TAP carrier. *Default*: Even
Data Bits	The number of data bits required for a connection by modem to a TAP paging terminal of this service provider. Choose `7` or `8`, according to the information provided by the TAP carrier. *Default*: `7`

Configure general paging setup. If parameters for **General Paging Setup** (**Paging Settings** in the control console) are not yet configured, configure them through the **Paging** option of the **Network** menu before you configure paging recipients.

General Paging Setting	Description
Message Delay	The time in seconds before paging begins when any on-battery event occurs. This setting determines how sensitive the paging function is to brief power disturbances. *Default*: 0; *Maximum*: 120
Repeat	The number of times that the Management Card will page a recipient. *Default*: 1 (The page will not be repeated); *Maximum*: 5 **NOTE:** This setting affects all configured paging recipients. (With an Out-of-Band Management Card, you can configure a different number of times for each paging recipient.)
Page Interval	The number of minutes between paging cycles (i.e. after all of the configured paging recipients have been paged and before the next retry begins). If the value is 0, the next cycle begins without a delay. *Default*: 1; *Maximum*: 10
Numeric Site ID	An 8-digit unique identification number for the UPS connected to this Network Management Card. • This number is sent as part of each paging message from this Management Card to a numeric (non-TAP) pager. • This number is sent as part of each paging message from this Management Card to a TAP pager, if `Numeric Site ID` is the value configured for Site ID Mode.
Site Name (TAP only)	An alphanumeric character string that identifies the UPS connected to this Network Management Card. This string is sent as part of each paging message from this Management Card to a TAP pager, if `Site Name` is the value configured for Site ID Mode. *Maximum*: 30 characters

General Paging Setting	Description
Site ID Mode (TAP only)	The type of identifier to be used in TAP paging messages. Choose from the following options: • IP Address • Host Name (the name of the host computer) • System Name (the name configured through the **Identification** option of the **System** menu) • The value configured as Numeric Site ID. • The value configured as Site Name. *Default*: IP Address

For the format of the messages displayed on each type of supported pager, see Paging message formats.

Configure Paging Recipients. You can configure parameters for up to four paging recipients.

1. Using the **Paging** option of the **Network** menu, select the recipient to configure, and set the following parameters for that recipient.

Recipient Parameter	Description
Name	Uniquely identifies this paging recipient. *Maximum length*: 20 characters *Default*: `Pager 1` through `Pager 4`
Access	Enables or disables paging to this recipient. *Default*: `Disabled`
Mode	The type of paging service that this pager uses. Select `Analog` for numeric-only pagers. Select `TAP` for pagers that use the TAP protocol, which is commonly used for cell phones and other paging devices that can receive text messages. *Default*: `Analog` **NOTE:** Changing the value specified for **Mode** changes the configurable parameters to those appropriate for that mode; step 2 describes the parameters for each mode.

2. Set the parameters that are specific to the mode you chose in step 1.

Parameter	Description
Analog Mode	
Dial String	A character string that the Management Card's modem uses to contact this paging recipient. The string must include the following: • The phone number or the pager • Any modem commands needed for tasks such as timing, waiting for a dial tone, accessing an external telephone line, and providing the pager Personal Identification Number (PIN). **Example:** 9,15555551234@ **NOTE:** The Management Card's modem supports only tone dialing, not pulse dialing.
Space Character	The specific character (*, @, #, or None) that this pager requires to display a space. A space is displayed between the site ID and the event code in the numeric message. *Default*: *
End String	A string of one to ten characters to be appended to the dial string. The end string ensures that the modem hangs up when it completes paging the recipient. An end string is needed only if the paging service has a menu for reviewing and leaving messages.
Send Out-of-Band Management Card event codes	Enables or disables automatic conversion of Network Management Card event codes to default Out-of-Band Management Card event codes. Enable this feature if your network has both Network Management Cards and Out-of-Band Management Cards, and you want paging notifications to use the same event codes regardless of which card reports the event. *Default*: Disabled **NOTE:** By default, Out-of-Band Management Cards enable paging for some events for which Network Management Cards do not. (By default, Network Management Cards enable paging for severe events only.) To ensure that paging is enabled for the same events throughout your system, you can enable or disable paging for individual events through the user interface of either card.

Parameter	Description
TAP mode	
TAP Carrier	An identifier (name string) for the TAP service provider that this pager uses.
Pager Number	The numeric identifier of this pager, i.e., its TAP ID. The TAP ID is usually the pager's phone number, but some TAP service providers require that the TAP ID also include the area code. If you are uncertain of the TAP ID, check with the TAP carrier.

To use the Network Management Card interface to enable or disable paging for an event, see Event Actions (Web Interface Only).

To understand how Network Management Card event codes are converted to default Out-of-Band Management Card event codes, see Conversion of event codes.

Test your paging configuration (Web interface only). When you finish configuring paging parameters, on the same Web page you can test your configuration by selecting a recipient and sending a test message.

Conversion of event codes. If **Send Out-of-Band Management Card Event Codes** is enabled for a paging recipient, any Network Management Card event code is automatically converted to a default Out-of-Band Management Card event code in paging notifications to that recipient.

Note

An Out-of-Band Management Card does not have event codes that correspond to the codes generated by the Integrated Environmental Monitor of an AP9618 Network Management Card *EM/MDM*. Therefore, codes 16 through 19 in the last of the following conversion tables have been created so that the Network Management Card event codes from the Integrated Environmental Monitor can be converted to codes that are compatible with numeric pagers.

For an explanation of the format of the message that a numeric pager will display when these converted event codes are used, see Paging message formats.

One of the following event codes is sent when the UPS starts up, shuts down, switches to battery operation, or has a battery-related problem.

Out-of-Band Management Card		Network Management Card	
Event Code	Event	Event Code	Event
0	UPS ON-BATTERY	0x0109	UPS: Switched to battery backup power.
1	AC FAIL/LOW BATTERY	0x010F	UPS: Battery power is low and will soon be exhausted.
2	UPS SHUT DOWN	0x0114	UPS: Turned off.
3	UPS ON-LINE	0x010A	UPS: Returned from battery backup power.
		0x0113	UPS: Turned on.
4	REPLACE BATTERY	0x0119	UPS: Batteries need replacement.

One of the following codes is sent when the UPS experiences a specific fault condition. Many of these fault conditions occur only with specific UPS models or specific UPS product lines.

Out-of-Band Management Card		**Network Management Card**	
Event Code	**Event**	**Event Code**	**Events**
5	UPS FAULT	0x011B, 0x0120, 0x011F, 0x012F, 0x0126, 0x0128, 0x012A	UPS events generated by faults of Smart-UPS or Matrix-UPS models.
		0x0201, 0x0203, 0x0205, 0x0207, 0x0209, 0x020B, 0x020D, 0x020F, 0x0211, 0x0213, 0x0215, 0x0217, 0x0219, 0x021B, 0x021D, 0x021F, 0x0221, 0x0223, 0x0225, 0x0227, 0x0229, 0x022B, 0x022D, 0x022F, 0x0231, 0x0233, 0x0235, 0x0237, 0x0239, 0x023B, 0x023D, 0x023F, 0x0242, 0x0244, 0x0246, 0x0248	UPS events generated by faults of Symmetra UPS models (single-phase only).
		0x0A01, 0x0A03, 0x0A05, 0x0A07, 0x0A09, 0x0A0B, 0x0A0D,0x0A0F, 0x0A11, 0x0A13, 0x0A15, 0x0A17, 0x0A19, 0x0A1B, 0x0A1D, 0x0A1F, 0x0A21, 0x0A23, 0x0A25, 0x0A27, 0x0A29, 0x0A2B, 0x0A2D, 0x0A2F, 0x0A31, 0x0A33, 0x0A35, 0x0A37, 0x0A39, 0x0A3B, 0x0A3D,0x0A3F, 0x0A41, 0x0A43, 0x0A45, 0x0A47, 0x0A49, 0x0A4B, 0x0A4D, 0x0A4F, 0x0A51, 0x0A53, 0x0A55, 0x0A57, 0x0A59, 0x0A5B, 0x0A5D, 0x0A5F, 0x0A61, 0x0A63, 0x0A65, 0x0A67, 0x0A69, 0x0A6B, 0x0A6D, 0x0A6F, 0x0A71, 0x0A73, 0x0A75, 0x0A77, 0x0A79, 0x0A7B, 0x0A7D, 0x0A7F	UPS events generated by faults of Symmetra, Symmetra 3-phase, and Silcon UPS models.

See also

For descriptions of the events relevant to a particular UPS model, see the event list in the Web interface of the Network Management Card connected to (or built into) that model. Select the **Actions** option of the **Events** menu, and then, on the **Event Action Configuration** page, click **Details....**

For descriptions of all events relevant to APC UPSs at the time this manual was last updated, see the file **.\doc\en\Events.pdf** on the APC Network Management Card *utility* CD. For subsequent updates to that Events.pdf file, go to the Software Downloads page of the APC Web site (**www.apcc.com/tools/download/**).

One of the following event codes is sent when communication with the UPS is lost, when the UPS switches to bypass operation, or when the UPS is overloaded.

Out-of-Band Management Card		**Network Management Card**	
Event Code	**Event**	**Event Code**	**Events**
6	LOST COM W/UPS	0x0102	UPS: Communications lost.
7	BYPASS/OVERLOAD	0x0103	UPS: Sensed a load greater than 100 percent of rated capacity.
		0x011C	UPS: In bypass due to user command via software or panel.
		0x011D	UPS: In bypass initiated by user.

One of the following event codes is sent when an environmental monitoring device (either the separate Environmental Monitoring Card or the Integrated Environmental Monitor of the Network Management Card) detects a problem or reports that a problem is resolved.

Out-of-Band Management Card		**Network Management Card**	
Event Code	**Event**	**Event Codes**	**Events †**
8	ZONE 1	0x0301	Environment: Contact 1 fault.
9	ZONE 2	0x0303	Environment: Contact 2 fault.
10	ZONE 3	0x0305	Environment: Contact 3 fault.
11	ZONE 4	0x0307	Environment: Contact 4 fault.
12	ZONES CLEARED	0x0302	Environment: Contact 1 fault cleared.
		0x0304	Environment: Contact 2 fault cleared.
		0x0306	Environment: Contact 3 fault cleared.
		0x0308	Environment: Contact 4 fault cleared.
13	PROBE 1	0x0309	Environment: Low temperature threshold violation on probe 1.
		0x030B	Environment: High temperature threshold violation on probe 1.
		0x030D	Environment: Low humidity threshold violation on probe 1.
		0x030F	Environment: High humidity threshold violation on probe 1.

† Generated by an Environmental Monitoring Card

Out-of-Band Management Card		Network Management Card	
Event Code	Event	Event Codes	Events †
14	PROBE 2	0x0311	Environment: Low temperature threshold violation on probe 2.
		0x0313	Environment: High temperature threshold violation on probe 2.
		0x0315	Environment: Low humidity threshold violation on probe 2.
		0x0317	Environment: High humidity threshold violation on probe 2.
15	PROBES CLEAR	0x030A	Environment: Low temperature threshold violation on probe 1 cleared.
		0x030C	Environment: High temperature threshold violation on probe 1 cleared.
		0x030E	Environment: Low humidity threshold violation on probe 1 cleared.
		0x0310	Environment: High humidity threshold violation on probe 1 cleared.
		0x0312	Environment: Low temperature threshold violation on probe 2 cleared.
		0x0314	Environment: High temperature threshold violation on probe 2 cleared.
		0x0316	Environment: Low humidity threshold violation on probe 2 cleared.
		0x0318	Environment: High humidity threshold violation on probe 2 cleared.

† Generated by an Environmental Monitoring Card

Event Code (Converted to Numeric format) and Event Name †		Network Management Card	
Event Code	**Event**	**Event Codes**	**Events**
16	INTERNAL ZONE	0x031B	Environment: Integrated contact fault.
17	INTERNAL ZONE CLEAR	0x031C	Environment: Integrated contact fault cleared.
18	INTERNAL PROBE	0x031D	Environment: Low temperature threshold violation on integrated probe.
		0x031F	Environment: High temperature threshold violation on integrated probe.
		0x0321	Environment: Low humidity threshold violation on integrated probe.
		0x0323	Environment: High humidity threshold violation on integrated probe.
19	INTERNAL PROBE CLEAR	0x031E	Environment: Low temperature threshold violation on integrated probe cleared.
		0x0320	Environment: High temperature threshold violation on integrated probe cleared.
		0x0322	Environment: Low humidity threshold violation on integrated probe cleared.
		0x0324	Environment: High humidity threshold violation on integrated probe cleared.

† The Out-of-Band Management Card has no event codes or event names for these events, which are generated by the Integrated Environmental Monitor of the AP9618 Network Management Card *EM/MDM*.

Paging message formats. The types of supported pagers display messages in one of the following formats (two analog formats and one TAP format):

Analog Mode	Format
Network Management Card event code format (for numeric pagers only)	[*site_ID*] [*space_character*] [*event_code*] • *site_ID*: A configurable 8-digit number to identify the location of the UPS. See Numeric Site ID. • *space_character*: The character that the pager requires to display a space. See Space Character. • *event_code:* A six-digit number, with the decimal form of the Network Management Card event type as the first three digits and the decimal form of the Network Management Card event number as the last three digits. **Example**: `636792 001007`
Out-of-Band Management Card event code format (for numeric pagers only)	[*site_ID*] [*space_character*] [*event_code*] • *site_ID*: A configurable 8-digit number to identify the location of the UPS. See Numeric Site ID. • *space_character*: The character that the pager requires to display a space. See Space Character. • *event_code*: A one- or two-digit number in the format of an Out-of-Band Management Card event code after conversion from a Network Management Card event code. See Conversion of event codes. **Example**: `752968 8`

TAP Mode	Format
For non-numeric pagers. Maximum message length: 160 characters.	*location_ID*:*severity*:*event_code*:*event_text* • *location_ID*: The IP address, host name, device name, numeric site ID, or site name that uniquely identifies the location of the UPS. *location_ID* must be the type of identifier configured as Site ID Mode in **Configure General Paging Settings**. • *severity*: The severity of the event (severe, warning, or informational). • *event_code*: The hexadecimal Network Management Card event code. • *event_text*: The Network Management Card event text. **Example**: `139.234.6.49:Severe:0x0107:UPS: Batteries Discharged`

System Menu

Introduction

Overview

Use the **System** menu to do the following tasks:

- Configure system identification, date and time settings, and access parameters for the Administrator, Device Manager, and Read Only User accounts.
- Synchronize the Management Card's real-time clock with a Network Time Protocol (NTP) server.
- Reset or restart the Management Card.
- Define the URL links available in the Web interface.
- Access hardware and firmware information about the Management Card.
- Set the units (Fahrenheit or Celsius) used for temperature displays.
- Configure dial-in access to the control console at an AP9618 Network Management Card using the Management Card's internal analog modem.

Note

Only an Administrator has access to the **System** menu.

Menu options

Unless noted, the following menu options are available in the control console and Web interface:

- User Manager
- Identification
- Date & Time
- Tools
- Modem (AP9618 control console)
- Preferences (Web interface)
- Links (Web interface)
- About System

Note

About System is an option of the **Help** menu in the Web interface.

Option Settings

User Manager

Use this option to define the access values shared by the control console and the Web interface, and the authentication used to access the Web interface.

Setting	Definition
Values affecting all users	
Auto Logout	The number of minutes (3 by default) before a user is automatically logged off because of inactivity.
Authentication	The **Basic** setting (default) causes the Web interface to use standard HTTP 1.1 login (base64-encoded passwords); **MD5** causes the Web interface to use an MD5-based authentication login. **NOTE:** To use a browser with MD5 authentication, Cookies must be enabled at a browser before it can be used with MD5 authentication.
Separate values for Administrator, Device Manager, and Read Only User	
User Name	The case-sensitive name (maximum of 10 characters) used by Administrator and Device Manager users to log on at the control console or Web interface and by the Read-Only User to log on at the Web interface. Default values are **apc** for **Administrator** users, **device** for **Device Manager** users, and **readonly** for the **Read Only User**.
Password	The case-sensitive password (maximum of 10 characters) always used to log on at the control console, but only used to log on to the Web interface when **Basic** is selected for the **Authentication** setting (**apc** is the default for the **Password** settings for the three account types). **NOTE:** A Read Only User cannot log on through the control console.
Authentication Phrase	The case-sensitive, 15-to-32 character phrase used to log on to the Web interface when MD5 is the **Authentication** setting. Default settings are: • **admin user phrase** for **Administrator** • **device user phrase** for **Device Manager** • **readonly user phrase** for **Read Only User**

Identification

Use this option to define the System **Name**, **Location**, and **Contact** values used by the Management Card's SNMP agent. The option's settings provide the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifications (OIDs).

For more information about the MIB-II OIDs, see the PowerNet® *SNMP Management Information Base (MIB) Reference Guide* (**.\doc\en\mibguide.pdf**) provided on the APC Network Management Card *utility* CD.

Date & Time

Use this option to set the time and date used by the Management Card. The option displays the current settings, and allows you to change those settings manually, or through a Network Time Protocol (NTP) Server.

Set Manually. Use this option in the Web interface, or **Manual** in the control console, to define the date and time for the Management Card.

Note

An **Apply Local Computer Time to** Network Management Card option, which is available in the Web interface only, sets these values to match the date and time settings of the computer you are using to access the Web interface.

Synchronize with Network Time Protocol (NTP) Server. Use this option, or **Network Time Protocol (NTP)** in the control console, to have an NTP Server update the date and time for the Management Card automatically.

Note

In the control console, use the **NTP Client** option to enable or disable (the default) the NTP Server updates. In the Web interface, use the **Set Manually** option to disable the updates.

Setting	Definition
Primary NTP Server	Identifies the IP address or domain name of the primary NTP server.
Secondary NTP Server	Identifies the IP address or domain name of the secondary NTP server, when a secondary server is available.
GMT Offset (Time Zone)	Defines the offset from Greenwich Mean Time (GMT) based on the Management Card's time zone.
Update Interval	Defines how often, in hours, the Management Card accesses the NTP Server for an update. The minimum is 1 hour; the maximum is 8760 hours (1 year). Use **Update Using NTP Now** to initiate an immediate update as well.

Tools

Initiating an action. Use this drop-down list in the Web interface or the equivalent menu options in the control console to restart the interface of the Management Card, to reset some or all of its configuration settings to their default values, or to delete SSH Host Keys and SSL Certificates.

Action	Definition
Reboot Management Interface	Restarts the interface of the Management Card.
Reset to Defaults	Resets all configuration settings. **NOTE:** For information about how this affects the **Boot mode** setting, see this table's description of **Reset Only TCP/IP to Defaults**.
Reset to Defaults Except TCP/IP	Resets all configuration settings except the TCP/IP settings.
Reset Only TCP/IP to Defaults	Resets the TCP/IP settings only. **NOTE:** WIth **Boot mode** set to **DHCP & BOOTP**, its default setting, the Management Card's TCP/IP settings must be defined by a DHCP or BOOTP server. See TCP/IP.
Delete SSH Host Keys and SSL Certificates	Removes any SSH host key and server certificate on the Management Card so that you can reconfigure these components of your security system.

Uploading an initialization file (Web interface only). To transfer configuration settings from a configured Management Card to the current Management Card, export the .ini file from the configured Management Card, select the **Tools** menu on the current Management Card, browse to the file, and click **Upload**. The current Management Card imports the file and uses it to set its own configuration The **Status** field reports the progress of the upload.

See How to Export Configuration Settings for information on the content of the .ini file, how to preserve comments you add to the file, and how to export settings to multiple Management Cards.

File Transfer (control console only). The **File Transfer** option of the **Tools** menu provides two methods for file transfer over the network and one for file transfer through a serial connection to the Management Card.

Option	Description
XMODEM	Allows you to transfer either an .ini file or a firmware upgrade file to a Management Card using a terminal-emulation program. This option is available only when you use a local connection to the control console. See Local access to the control console.
FTP Client	Use one of these two option to transfer either an .ini file or a firmware upgrade file from an FTP or TFTP server of your organization (company, agency, or department) to the current Management Card. These options assume that your organization has a centralized system for configuring or upgrading APC Management Cards. For **FTP Client**, you are prompted for a user name and password. For either option, you are then prompted for the server address and the file to transfer. After you supply that required information, the Management Card transfers the file.
TFTP Client	

Preferences (Web interface)

Use this option to define whether temperature values are displayed as Fahrenheit or Celsius in the Web interface and the control console.

Links (Web interface)

Use this option to modify the links to APC Web pages.

Setting	**Definition**
User Links	
Name	Defines the link names that appear in the **Links** menu (by default, **APC's Web Site**, **Testdrive Demo**, and **APC Monitoring**).
URL	Defines the URL addresses used by the links. By default, the following URL addresses are used: • **http://www.apc.com** (**APC's Web Site**) • **http://testdrive.apc.com** (**Testdrive Demo**) • **http://rms.apc.com** (**APC Monitoring**) **NOTE:** For information about these pages see Links menu.
Access Links	
APC Home Page	Defines the URL address used by the APC logo at the top of all Web interface pages (by default, **http://www.apc.com**).

Modem (AP9618 control console)

Use this option, which is available in the AP9618 Network Management Card's control console only, to configure dial-in access to the control console using the Management Card's internal analog modem.

Setting	Definition
Console Dial-In	Enables (by default) or disables dial-in access to the control console through the analog modem.
Initialization	Defines the initialization string used to ensure proper operation of the modem and consistent communication between the modem and the Management Card. This string is sent to the Management Card's internal modem every time the Management Card restarts, or when a setting is changed and accepted.
Country Code	Identifies the country in which the modem is used to match the modem's operation to that country's telephone-system standards.
Terminal Interface	Allows an advanced user to send commands directly to the modem and view the modem's response, using a serial, terminal-interface session at a baud rate of 38400. When CTRL+A is used to end the session, the modem is reset to use the **Initialization** setting.
Dialback	Disables (by default) or enables dial-back. With dial-back enabled, when the user whose telephone number is configured as **Dialback String** dials in to the Management Card remotely, the Management Card terminates the call immediately and calls that user's modem back. • Dial-back ensures that a dial-in control console session can occur only from the phone number configured as **Dialback String**, providing protection from unauthorized access. • The cost of the subsequent Control Console session is charged to your company or agency at its telephone calling rate and not to the user at the user's telephone calling rate.
Dialback String	The modem phone number to call back when **Dialback** is enabled. Include any modem commands needed for tasks such as timing, waiting for a dial tone, or accessing an external telephone line. The default (and sample) dial string is 9,5551234.

About System

This option identifies hardware information for the Management Card, including **Model Number**, **Serial Number**, **Manufacture Date**, **Hardware Revision**, **MAC Address**, and **Flash Type.**

The hardware information will never change. For example, if you use an AP9168U upgrade kit to convert an AP9617 Network Management Card *EX* to an AP9618 Network Management Card *EM/MDM*, the **About System** option still reports **AP9617** for that Management Card's model number.

Note

In the Web interface, except for **Flash Type**, this hardware information is reported by the **About System** option in the **Help** menu.

UPS Menu

Introduction

Overview

In the Web interface, the UPS menu is in the navigation menu; in the control console, you access the UPS menu through the **Device Manager** option in the **Control Console** menu. The menu is named with the model name of the UPS you are using.

UPS menu options

The UPS menu options and the information they provide vary by UPS model.

For information about the UPS menu options available in both the control console and the Web interface, see the following:

- UPS Status
- Diagnostics
- Control
- Configuration
- Outlet Groups (Smart-UPS XLM)
- PowerChute (UPS PowerChute Network Shutdown)
- Module Status (Symmetra UPS or Symmetra PX UPS)
- Scheduling UPS Shutdown (Web interface only)
- Sync Control

Note

A Silcon UPS has no **Diagnostics** or **Scheduling** options.

UPS Status

Overview

The **Status** options provide access to the information described in the following sections:

- Detailed UPS Status
- Utility Power Status
- Output Power Status
- Fault Tolerance (Symmetra or Symmetra PX UPS)
- Battery Status
- Intelligence Module (Smart-UPS VT)
- About UPS

For a Silcon UPS, the “Status of UPS” page in the Web interface includes the **View the refreshing status page** hyperlink described in Configure Parallel UPS Parameters (Silcon UPS only).

Detailed UPS Status

In the Web interface, use the **Status** option in the UPS menu to access the following UPS status information; in the control console, this status information is listed above the UPS menu.

- The current status of the UPS:
  - – Whether the UPS is online, and whether any alarms are present

    For a list of the UPS events that can be reported as part of the UPS status, see "Event List" page.

  - – For a Smart-UPS XLM model (when UPS output is on), the status of each outlet group (**On** or **Off**)
    - In the Web interface, outlet status is displayed wherever UPS status is displayed. If a command is pending for the outlet group, the outlet group's status is displayed in orange.
    - In the control console, outlet status is displayed when you choose any **Control** option of the UPS menu as well as above the UPS menu itself. If a command is pending for the outlet group, the outlet group's status is displayed with an asterisk (**On*** or **Off***).

  Note: In the control console, the **Detailed Status** option (Smart-UPS or Matrix-UPS) or **Detailed UPS Information** option (Symmetra or Silcon UPS) accesses expanded descriptions of the UPS status.

    - For Symmetra UPS models, the **Faults & Alarms** option accesses descriptions of any faults or alarms reported.
    - For information about the conditions that are mapped to the non-specific faults that a Silcon UPS can report, see the file **dp3etrap.pdf** in the **.\help\dp3e\** folder on the APC Network Management Card *utility* CD

- The reason for the last transfer to battery power at the UPS
- The internal temperature of the UPS

- The runtime that is available currently to the UPS
- The values described in Utility Power Status, Output Power Status, and Battery Status
- The Fault tolerance parameters described in Fault Tolerance (Symmetra or Symmetra PX UPS)

Utility Power Status

Footnotes indicate which utility-power fields are shared by which UPS models. (If no footnote is used, all UPS models report that value.)

Note

A multi-phase UPS (Smart-UPS VT, some models of Symmetra UPS, or Silcon UPS) identifies the values for all supporting phases.

Status Field	Definition
Bypass Input Voltage[1]	The AC voltage (VAC) used when the UPS is in bypass mode.
Input Current[1]	The current, in Amps, supplied by the input voltage.
Input Frequency[2]	The input voltage's frequency, in Hertz (Hz). **NOTE:** In the control console for Smart-UPS or Matrix-UPS, the **Operating Frequency** field reports the frequency value shared by the input and output voltages.
Input Voltage	The AC voltage (VAC) being input to the UPS.
Minimum Line Voltage	The lowest AC voltage input to the UPS during the previous minute of operation.
Maximum Line Voltage	The highest AC voltage input to the UPS during the previous minute of operation.

[1] Smart-UPS VT, Symmetra PX UPS and Silcon UPS models
[2] Smart-UPS, Matrix-UPS, or Symmetra UPS models

Output Power Status

Footnotes indicate which output-power fields are shared by which UPS models.

The Smart-UPS product line has a wide variety of models. If a status field is listed for Smart-UPS in the table, it may be supported on only some Smart-UPS models.

Only the status field **Output Voltage** is shared by all UPS models.

Note

A multi-phase UPS (Smart-UPS VT, some models of Symmetra UPS, or Silcon UPS) identifies the values for all supporting phases.

Status Field	Definition
Load Current[1, 2] or Output Current[3]	The current, in Amps, supplied to the load.
Load Power[1, 2]	The UPS load as a percentage of available Watts.
Apparent Load Power[1, 2]	The UPS load as a percentage of available VA.
Output Frequency[4]	The frequency, in Hz, used by the output voltage. In the control console for Smart-UPS or Matrix-UPS, the **Operating Frequency** field reports the frequency value shared by the input and output voltages.
Output kVA[5] or Output Power[6]	The load placed on each phase by the attached equipment, in total kVA.
Output Power Percentage[6]	The load placed on each phase by the attached equipment, expressed as a percentage of the available kVA.
Output VA at n+0[7]	The load placed on each phase by the attached equipment, as a percentage of the VA available with no redundancy.
Output VA at n+1[7]	The load placed on each phase by the attached equipment, as a percentage of the VA available with the identified redundancy.
Output Voltage	The AC voltage the UPS is providing to its load.
Output Watts at n+0[7] Output Percent Load[9]	The load placed on each phase by the attached equipment, as a percentage of the Watts available with no redundancy.
Output Watts at n+1[7]	The load placed on each phase by the attached equipment, as a percentage of the Watts available with the identified redundancy.
Peak Output Current[8]	The highest current, in Amps, output by each phase.

[1] Matrix-UPS
[2] Smart-UPS
[3] Smart-UPS VT, Symmetra, Symmetra PX UPS, or Silcon UPS
[4] Smart-UPS, Matrix-UPS, or Symmetra UPS
[5] Smart-UPS VT or Symmetra PX UPS
[6] Silcon UPS
[7] Symmetra or Symmetra PX UPS
[8] Symmetra PX UPS or Silcon UPS
[9] Smart-UPS VT

Fault Tolerance (Symmetra or Symmetra PX UPS)

Note

In the control console, use the **Detailed UPS Information** option to access the fault tolerance status.

Status Field	Definition
Present kVA Capacity	The maximum load that the Symmetra can support.
Redundancy	The number of power modules which can fail or be removed without causing the Symmetra to switch to bypass.

Battery Status

Footnotes indicate which output-power fields are shared by which UPS models. Only the status field **Runtime Remaining** is shared by all UPS models.

Status Field	Definition
Battery Capacity[1]	How much of the UPS battery capacity is available to support the attached equipment.
Battery Current[2]	The current being output from the battery.
Battery Voltage[3], Actual Battery Voltage[2], or Actual Battery Bus Voltage[4]	The available DC power.
Calibration Date[1]	When the last runtime calibration was performed.
Calibration Result[1]	The result of the last runtime calibration.
Nominal Battery Voltage[5]	The basic voltage range that the battery needs to supply when the UPS uses its battery for output power. This field appears only in the Web interface.
Number of Bad Batteries[1]	How many UPS batteries need replacing (reported only when the UPS has at least one external battery).
Number of Batteries[3] or Number of External Batteries[6]	How many batteries the UPS has.
Runtime Remaining	How long the UPS can use battery power to support its attached equipment.
Self-Test Result[1]	The result of the last self-test.

[1] Smart-UPS, Matrix-UPS, Symmetra, or Symmetra PX UPS
[2] Smart-UPS VT, Symmetra PX UPS, or Silcon UPS
[3] Smart-UPS or Matrix-UPS
[4] Symmetra PX UPS
[5] Smart-UPS VT, Symmetra, Symmetra PX UPS, or Silcon UPS
[6] Symmetra or Symmetra PX UPS
[7] Smart-UPS VT
[8] Symmetra LX

Status Field	Definition
Self-Test Date[1]	When the last self-test was performed.
External Battery Cabinet Amp-Hour Rating[7, 8]	The battery cabinet Amp-Hour rating of an external battery source.
UPS Position[8]	The physical orientation of the UPS, rack or tower.

1 Smart-UPS, Matrix-UPS, Symmetra, or Symmetra PX UPS
2 Smart-UPS VT, Symmetra PX UPS, or Silcon UPS
3 Smart-UPS or Matrix-UPS
4 Symmetra PX UPS
5 Smart-UPS VT, Symmetra, Symmetra PX UPS, or Silcon UPS
6 Symmetra or Symmetra PX UPS
7 Smart-UPS VT
8 Symmetra LX

Intelligence Module (Smart-UPS VT)

This option displays information in the following fields: Firmware Revision, Manufacture Date, Serial Number, and Hardware Revision.

About UPS

This option displays information in the following fields: Model Number, Firmware Revision, Manufacture Date, and Serial Number.

Diagnostics

Overview

There are two types of diagnostics options you can use with all UPS models except a Silcon UPS, which has no diagnostic options:

- Options which cause a specified test to occur immediately
- A scheduling option which controls when a UPS self-test occurs

Diagnostic tests

In the Web interface, use the **Diagnostics** option of the UPS menu to perform diagnostic tests or to view the results of the last self-test or runtime calibration.

Note

In the control console, the diagnostics options are in the **Control** menu.

Smart-UPS, Matrix-UPS, or Symmetra UPS. You can use diagnostics options to perform the following tests.

Note

For the results of the last self-test and last runtime calibration:

- In the Web interface, use the "Diagnostics" page.
- In the control console, use the option **Detailed Status** (Smart-UPS or Matrix-UPS models) or **Detailed UPS Information** (Symmetra or Silcon UPS models).

Test	**Definition**
Self-Test	Perform a self-test of the UPS.
Simulate Power Failure	Causes the UPS to test its ability to switch to battery operation.
Start/Stop Runtime Calibration	Initiates (or cancels) a runtime calibration, a process which calculates how much runtime the UPS has available. **NOTE:** You can perform a runtime calibration only when the battery is at 100% capacity.
Test UPS Alarm (Smart-UPS or Matrix-UPS)	Causes a Matrix-UPS to generate an alarm tone, and a Smart-UPS to generate an alarm tone and flash its front panel lights. If the Smart-UPS is a member of a Synchronized Control Group: • In the Web interface, this option always tests the alarms of all enabled members of the group. • In the control console, you are prompted to choose whether to apply the action to the initiating UPS or to all members of the group. • In SNMP, you can set the OID **upsAdvControlFlashAndBeep** to either option: **flashAndBeep (2)** to test the alarm of an individual UPS or **flashAndBeepSyncGroup (3)** to test the alarms of all enabled group members.

Symmetra PX UPS. Use buttons on the "Diagnostics" page in the Web interface to perform self-tests (**Tests...**) or runtime calibrations (**Calibrate...**).

Note

For the results of the last self-test and last runtime calibration, and the status of intelligence modules, power modules, batteries, and the communication bus and subsystems:

- In the Web interface, use the "Diagnostics" page.
- In the control console, use the **Detailed UPS Information** option.

Scheduled UPS self-tests

To schedule a self-test:

- In the Web interface, select **Diagnostics** on the UPS menu, then use the **Auto Self-Test** option.
- In the control console, from the UPS menu:
  - For Symmetra and Symmetra PX UPS models, select **Scheduled Tests**.
  - For Smart-UPS or Matrix-UPS models, select **Configuration**, **General**, and **Self-Test Schedule**.

The scheduling option allows you to control when a UPS self-test occurs. The available selections are **Never**, **UPS Startup**, **Every 7 Days**, or **Every 14 Days**.

Control

Initiating a UPS Control option

You can initiate a UPS Control option in either of these ways:

- For the UPS of the initiating Management Card only.
  - In the Web interface, select **No** for **Apply to Sync Group?**
  - In the control console, type **NO** (in uppercase) in response to the question **Apply command to all SCG members?**
- For all members of the Synchronized Control Group to which this Management Card belongs (if the option is allowed for Synchronized Control Groups).
  - In the Web interface, select **Yes** for **Apply to Sync Group?**
  - In the control console, press ENTER in response to the question **Apply command to all SCG members?**

Note

The option to apply an action to a Synchronized Control Group is displayed only if this Management Card is an active (enabled) member of a Synchronized Control Group.

The following guidelines apply to Synchronized Control Groups:

- All UPSs in a Synchronized Control Group must be the same model.
- Synchronized Control Groups are supported for most UPS models of the Smart-UPS and Symmetra UPS product lines. Any Smart-UPS or Symmetra UPS with a card slot that accepts a Network Management Card supports Synchronized Control Groups.
- In a Synchronized Control Group of Symmetra 3-phase UPSs, the shutdown mode setting must be either normal or secure for each UPS.

To configure a Management Card to be a member of a Synchronized Control Group, see Sync Control.

The synchronization process . If you apply an action to the Synchronization Control Group, the UPSs with management cards that are enabled group members behave as follows:

- Each UPS receives the command regardless of its output status, even if it is in a low-battery state.
- The action uses the delay periods (such as **Shutdown Delay**, **Sleep Time**, and **Return Delay)** that are configured for the initiating UPS.
- When the action begins, a UPS that is unable to participate retains its present output status while the other UPSs in the group perform the action. If a UPS is already in the output state that the action requires (e.g., a UPS is already off when the **Reboot UPS** action starts), that UPS logs an event, but performs the rest of the action, if any.
- All UPSs participating in the action synchronize their performance of the action (within a one-second time period under ideal conditions for Smart-UPS, but sometimes longer, especially for Symmetra UPSs).
- In reboot and sleep actions:
  - Immediately before the initiating UPS begins its **Return Delay**, by default it waits up to 120 seconds (its configurable **Power Synchronized Delay**) for any UPS that does not have input power to regain that power. Any UPS that fails to regain input power within the **Power Synchronized Delay** does not participate in the synchronized restart, but instead waits until its own input power returns before restarting.
  - The LEDs on the front of the UPS do not sequence their lights as they do for a normal (not synchronized) reboot or sleep action.
- UPS status and events are reported in the same way for synchronized actions as for actions on individual UPSs.

For more information about the delays and required battery capacity settings in the following table, see Configuration and Sync Control.

Actions (for a single UPS and Synchronized Control Groups). Use the actions described in the table on the next several pages for individual UPSs and for Synchronized Control Groups, within these guidelines:

- All actions except **Put UPS in Bypass** and **Take UPS Off Bypass**:
  - These actions are available for Synchronized Control Groups of Symmetra UPS or Smart-UPS models.
  - These actions are available for all individual APC UPSs except Silcon UPS models.

    To control a Silcon UPS, see Control options for Silcon UPS.

- **Put UPS in Bypass** and **Take UPS Off Bypass**:
  - These actions are available only for individual UPSs, not for Synchronized Control Groups.
  - These actions are available only for Matrix-UPS, Symmetra UPS, and some Smart-UPS models.

For descriptions of the UPS Control options **Self-Test**, **Simulate Power Failure**, **Start/Stop Runtime Calibration**, and **Test UPS Alarm**, see Diagnostic tests.

Action	Definition
Turn UPS On (control console)	This action turns on power at the UPS. • For a Smart-UPS XLM model, which has outlet groups, this action then turns on the outlet groups according to the value configured for **Power On Delay** for each group. See Delay Settings. • For a Synchronized Control Group, after a delay of a few seconds, the action turns on all enabled group members that have input power.
Turn UPS Off	This action turns off the output power of the UPS and (for a Smart-UPS XLM) all its outlet groups immediately, without a shutdown delay. The UPS and all its outlet groups remain off until you turn on its power again. If the UPS is a member of a Synchronized Control Group, this action turns off power at all UPSs that are enabled members of the group. No **Shutdown Delay** value is used. The UPSs turn off after a few seconds, and they remain off until you turn on their power again. See Shutdown Parameters. **NOTE:** For a synchronized turn-off action that uses the **Shutdown Delay** of the initiating UPS, use SNMP. Set the value **turnUpsSyncGroupOffAfterDelay (5)** for the **upsAdvControlUpsOff** OID.
Turn UPS Off Gracefully[1] (control console)	This action turns off outlet power of the UPS and (for a Smart-UPS XLM model) all its outlet groups after the UPS's **Maximum Shutdown Time** plus two minutes, and its **Shutdown Delay**. See Maximum-Shutdown-Time negotiation and Shutdown Parameters. For a Synchronized Control Group, the action is performed using the delays configured for the group member that initiated the action.

[1] When you select **Yes** for the Web interface's **Signal servers** option, initiating a **Turn UPS Off**, **Reboot UPS**, or **Put UPS To Sleep** action is equivalent to selecting **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, or **Put UPS To Sleep Gracefully** in the control console.

Action	Definition
Reboot UPS	This option restarts the attached equipment by doing the following: • Turns off power at the UPS after the **Shutdown Delay.** • Turns on power at the UPS after the UPS battery capacity returns to at least the percentage configured for **Return Battery Capacity** and the UPS waits the time specified as **Return Delay**. See Shutdown Parameters. • For a Smart-UPS XLM model with outlet groups configured, a **Power On Delay** occurs after the UPS turns on and before an outlet group turns on. You configure the **Power On Delay** for each outlet group through the **Outlet Control** option of the UPS menu. See Delay Settings. For a Synchronized Control Group action: • This option turns off power at the UPSs that are enabled group members after waiting the time configured as the initiating UPSs **Shutdown Delay**. See Shutdown Parameters. • The initiating UPS then waits up to the number of seconds specified as **Power Synchronized Delay** to allow time for group members to regain input power. If all group members have already regained input power, this delay is omitted. If all group members regain input power during the delay, the remainder of the delay is cancelled. To configure **Power Synchronized Delay**, see Configure Synchronized Control. • The **Return Delay** then starts when the initiating UPS is at its configured **Return Battery Capacity**. See Shutdown Parameters. • The **Return Battery Capacity** of the initiating UPS is also required of group members, but you can reduce the capacity required of a group member by configuring that member's **Return Battery Capacity Offset** (set at 10% by default). For example, if the initiator's **Return Battery Capacity** is set at 50%, and a member's **Return Battery Capacity Offset** is set to 5%, that member's battery capacity will need to be at only 45% for that member to reboot. See Configure Synchronized Control.

[1] When you select **Yes** for the Web interface's **Signal servers** option, initiating a **Turn UPS Off**, **Reboot UPS**, or **Put UPS To Sleep** action is equivalent to selecting **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, or **Put UPS To Sleep Gracefully** in the control console.

Action	Definition
Reboot UPS Gracefully[1] (control console)	• This action is performed similarly to the **Reboot UPS** action, but with an additional delay before the shutdown portion of the action. The attached equipment shuts down only after the UPS (or the initiating UPS for a Synchronized Control Group action) waits the **Maximum Shutdown Time** plus two minutes. For information about how the **Maximum Shutdown Time** is determined, see Maximum-Shutdown-Time negotiation. • For a Smart-UPS XLM model with outlet groups configured, a **Power On Delay** occurs after the UPS turns on and before an outlet group turns on. You configure the **Power On Delay** for each outlet group through the **Outlet Control** option of the UPS menu. See Delay Settings.
Put UPS To Sleep	This option puts the UPS into sleep mode by turning off its output power for a defined period of time, as follows: • The UPS turns off output power after waiting the time configured as its **Shutdown Delay**. See Shutdown Parameters. • When input power returns, the UPS turns on output power after two configured periods of time: its **Sleep Time** and **Return Delay**. See Shutdown Parameters. • For a synchronized control group action, the Management Card of the UPS initiating the action waits up to the number of seconds configured as its **Power Synchronized Delay** for enabled group members to regain input power before it starts the **Return Delay**. If all group members have already regained input power, the **Power Synchronized Delay** is omitted. If all group members regain input power during the delay, the remainder of the delay is cancelled. See Configure Synchronized Control.

[1] When you select **Yes** for the Web interface's **Signal servers** option, initiating a **Turn UPS Off**, **Reboot UPS**, or **Put UPS To Sleep** action is equivalent to selecting **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, or **Put UPS To Sleep Gracefully** in the control console.

Action	Definition
Put UPS To Sleep Gracefully[1] (control console)	This action puts the UPS into sleep mode (turns off power for a defined period of time), as follows: • The UPS turns off output power after waiting the delay time configured as its **Maximum Shutdown Time** plus 2 minutes (to allow time for PowerChute Network Shutdown to shut down its server safely) and its **Shutdown Delay**. See Maximum-Shutdown-Time negotiation and Shutdown Parameters. • When input power returns, the UPS turns on output power after two configured periods of time: its **Sleep Time** and **Return Delay**. See Shutdown Parameters. • For a synchronized control group action, the Management Card of the UPS initiating the action waits up to the number of seconds configured as its **Power Synchronized Delay** for enabled group members to regain input power before it starts the **Return Delay**. If all group members have already regained input power, the **Power Synchronized Delay** is omitted. If all group members regain input power during the delay, the remainder of the delay is cancelled. See Configure Synchronized Control.
Put UPS In Bypass Take UPS Off Bypass	Controls the use of bypass mode, which allows maintenance to be performed at a Matrix-UPS, a Symmetra UPS, and some Smart-UPS models without turning off power at the UPS.

[1] When you select **Yes** for the Web interface's **Signal servers** option, initiating a **Turn UPS Off**, **Reboot UPS**, or **Put UPS To Sleep** action is equivalent to selecting **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, or **Put UPS To Sleep Gracefully** in the control console.

Outlet group behavior when you turn on the UPS. How the outlet groups of a Smart-UPS XLM model turn on depends on how they are configured and how you turn the UPS on or off.

- Until you configure the following actions and their related delays, when you turn on the UPS output, any outlet group that is off turns on by default and applies power to all devices attached to the outlets in that group.
- After you configure the actions and delays:
  - The actions and delays control how outlet groups turn on and off when you turn the UPS on or off from the user interfaces of the Network Management Card (the Web interface or control console).
  - When you turn on the UPS from its front panel, each group turns on after the number of seconds configured for **Power On Delay**.

Outlet group behavior when you turn off the UPS. When you turn a Smart-UPS XLM model off at its front panel, all outlets turn off immediately.

Control options for Silcon UPS. By default, no control options are available for Silcon UPS.

To use control options for a Silcon UPS, you must enable the **Accept Remote Turn Off Commands** option, available in the control console's **UPS Control** menu only when you use a local, serial connection to access the control console.

To use a serial connection, see Local access to the control console.

When **Accept Remote Turn Off Commands** is enabled:

- Two control options, **Turn UPS Off** and **Turn UPS Off Gracefully**, become available for a Silcon UPS
- **Disable Remote Turn Off Commands** on the **UPS Control** menu at the Web interface and control console allow you to disable using the Management Card to turn off the Silcon UPS.

How to control outlet group actions

Initiating an action. While the output of the Smart-UPS XLM model is on, select the **Control** option of the UPS menu to turn on, turn off, or restart any outlet group, with or without a delay.

- In the Web interface, these actions are under the heading **Initiate an Outlet Group control action**.
- In the control console, choose the sub-menu option **Outlet Groups**.

To configure any of the three delay values that the following actions use, see Delay Settings.

To override the turning on of outlet groups during the **Delayed On**, **Reboot**, or **Delayed Reboot** action, check-mark the **Never** box when configuring the **Power On Delay**, as described in Delay Settings. When that box is check-marked, the only action that turns on outlet groups is the **Immediate on** action.

Action	**Definition**
Immediate on	Turn on the outlet group immediately.
Delayed on	Turn on the outlet group after the number of seconds configured for **Power On Delay**.
Immediate off	Turn off the outlet group immediately.
Delayed off	Turn off the outlet group after the number of seconds configured for **Power Off Delay**.
Reboot	Turn the outlet group off immediately, then turn it on after the number of seconds configured for **Reboot Duration** and **Power On Delay**.
Delayed reboot	Turn the outlet group off after the number of seconds configured for **Power Off Delay**, then turn it on after the number of seconds configured for **Reboot Duration** and **Power On Delay**.

Outlet Group Events and Traps. A change in the state of any outlet group generates the event **UPS: Outlet Group turned on** with a default severity level of Informational, or **UPS: Outlet Group turned off** with a default severity level of Warning.The event messages are “UPS: Outlet Group *group_number*, *group_name*, *action* due to *reason*” and “UPS: Outlet Group *group_number*, *group name*, *action* due to *reason*”. For example:

```
UPS: Outlet Group 1, Web Server, turned on due to user
control.
```

```
UPS: Outlet Group 3, Printer, turned off due to line fail.
```

By default, each of these events generates an event log entry, an e-mail notification, and a Syslog message.

If you configure trap receivers for these events, SNMP trap 298 is generated when an outlet group turns on and SNMP trap 299 is generated when an outlet group turns off, with the event messages as trap arguments and with the default severity levels the same as for the events.

Configuration

Overview

The UPS menu's **Configuration** option provides access to the configurable parameters described in the following sections:

- Utility Line Settings
- Alarm Thresholds (Symmetra UPS or Symmetra PX UPS)
- Shutdown Parameters
- General Settings (Configuration)
- Reset UPS Defaults
- Configure Parallel UPS Parameters (Silcon UPS only)

Utility Line Settings

This **Configuration** menu option is available to all UPS models except a Silcon UPS. The available settings differ based on the UPS model.

Smart-UPS or Matrix-UPS. Not all **Utility Line** settings are available for all Smart-UPS and Matrix-UPS models, and each setting's selections can differ by UPS model.

Setting	Definition
Output Voltage	The nominal AC voltage level for the UPS output.
High Transfer Voltage	The upper limit of acceptable input voltage. When the input reaches this value: • Matrix-UPS switches to battery operation. • Smart-UPS starts to use its AVR Trim feature.
Low Transfer Voltage	The lower limit of acceptable input voltage. When the input reaches this value, Smart-UPS starts to use its AVR Boost feature or switches to battery operation if it does not have this feature. **NOTE:** For Matrix-UPS, this setting cannot be changed.
Bypass Upper Voltage	The input voltage above which the UPS cannot switch to bypass mode.
Bypass Lower Voltage	The input voltage below which the UPS cannot switch to bypass mode.
Vout Reporting (Matrix-UPS)	How Matrix-UPS scales its output voltage readings.
Sensitivity	How sensitive the UPS will be to distortions in the input voltage. **NOTE:** Matrix-UPS always uses the **Automatic** setting.
Output Frequency Range	Defines the nominal value for the frequency used by the output voltage.

Symmetra or Symmetra PX UPS. The following table describes the **Utility Line** settings for a Symmetra UPS. A Symmetra PX UPS uses only the settings **Output Frequency Range** and **If UPS fails**.

Setting	Definition
Output Voltage	Defines the nominal AC voltage level for the UPS output.
Vout Reporting	Defines how the UPS scales its output voltage readings.
Output Frequency Range	Defines the nominal value for the frequency used by the output voltage.
If UPS fails	Defines how the UPS will respond if it cannot continue to provide output power, and frequency or voltage is out of range.

Alarm Thresholds (Symmetra UPS or Symmetra PX UPS)

The following table describes the **Alarm Thresholds** settings for the Symmetra UPS or Symmetra PX UPS.

Threshold	Definition
Alarm if Redundancy Under	Defines the redundancy below which an alarm occurs.
Alarm if Load Over	Defines the maximum equipment load that the UPS will support without generating an alarm.
Alarm If Runtime Under	Defines the amount of runtime below which an alarm occurs.

Shutdown Parameters

All of the following settings are available with Smart-UPS, Matrix-UPS, Symmetra UPS, and Symmetra PX UPS models. A Silcon UPS uses only the **Low-Battery Duration**, **Maximum Shutdown Time**, and **Shutdown Delay** settings (under **Shutdown Behavior Settings**).

Note

In the control console, use the **Battery** option in the **Configuration** menu to access the **Return Battery Capacity** setting.

Action	**Definition**
Return Battery Capacity	Defines the minimum battery capacity required before the UPS turns on after a shutdown that was caused by a power failure. **NOTE:** The UPS must also wait the time defined by the **Return Delay** setting before it can turn on.
Low-Battery Duration	Defines how long the UPS can continue to run on battery power after a low-battery condition occurs. **NOTE:** This setting also defines the time available for PowerChute to safely shut down its server in response to the **Control** menu options **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, and **Put UPS To Sleep Gracefully**.
Maximum Shutdown Time (Web interface only)	Reports the delay that is defined by the **Maximum Shutdown Time** setting for the PowerChute Network Shutdown feature. **NOTE:** For information about the PowerChute Network Shutdown feature, see PowerChute (UPS PowerChute Network Shutdown); for information about how the **Maximum Shutdown Time** is determined, see Maximum-Shutdown-Time negotiation.
Shutdown Delay	Defines how long the UPS waits before it shuts down in response to a turn-off command.

Action	**Definition**
Return Delay	Defines how long the UPS waits before it turns on after a shutdown that was caused by a power failure. **NOTE:** The UPS must also have the capacity specified by the **Return Battery Capacity** setting before it can turn on.
Sleep Time	Defines how long the UPS sleeps (keeps its output power turned off) when you use either of the **Control** menu’s sleep options (**Put UPS To Sleep** or **Put UPS To Sleep Gracefully**). **NOTE:** This setting also is in the “Control” page of the Web interface.

General Settings (Configuration)

Four **General Settings** are available for Smart-UPS. The first two settings (**UPS Name** and **Last Battery Replacement**) are available for all other UPS models.

Note In the control console, use the **Battery** option in the **Configuration** menu to access the **Last Battery Replacement** and **External Batteries** settings.

Setting	Definition
UPS Name	Defines the name of the UPS.
Last Battery Replacement	Defines the date of the most recent UPS battery replacement. **NOTE:** Use *mm/dd/yy* format.
Self-Test Schedule (control console only)	Schedules when and how frequently a UPS self-test occurs. See Scheduled UPS self-tests.
Audible Alarm	Defines when Smart-UPS generates an alarm in response to switching to battery operation.
External Batteries	Defines how many external battery packs are connected to Smart-UPS XL. **NOTE:** Smart-UPS XL models cannot automatically sense and report the number of connected battery packs.
Simple Signal Shutdowns	When enabled, allows simple-signalling shutdown through PowerChute Network Shutdown.
External Battery Cabinet Amp-Hour Rating[1, 2]	The battery cabinet Amp-Hour rating of an external battery source.
UPS Position[2]	The physical orientation of the UPS, rack or tower.

[1] Smart-UPS VT
[2] Symmetra LX

Reset UPS Defaults

This option resets the UPS to use the default EEPROM values.

Caution

BEFORE YOU USE THIS OPTION, MAKE SURE THAT RESETTING THE EEPROM VALUES WILL NOT ADVERSELY AFFECT THE LOAD EQUIPMENT OR ANY SHUTDOWN SEQUENCE.

Configure Parallel UPS Parameters (Silcon UPS only)

Use this option, available only in the Web interface, to identify up to nine different Silcon UPSs that you can then access through the hyperlink, **View the refreshing status page**, in the "Status for UPS" page.

Setting	Definition
IP Address	Identifies the IP address of the Management Card of the Silcon UPS to be monitored.
Monitor Name	Identifies by name the Silcon UPS to be monitored.

Outlet Groups (Smart-UPS XLM)

Overview

The UPS provides AC output to three outlet groups (groups of one or more AC outlets). By using the network interface to control each outlet group remotely, you can start or stop devices sequentially and restart locked devices.

The UPS menu's **Outlet Groups** option provides access to the configurable parameters described in the following sections:

- Delay Settings
- General Settings (Outlet Groups)
- Automatic Load Shedding for Outlet Groups (Web interface only)

Delay Settings

In the Web interface or control console, you can set the following delays for each outlet group. The minimum value for each delay is 0 seconds, and the maximum value is 600 seconds. For information on the actions that use these delays, see How to control outlet group actions.

Delay	Definition
Power On Delay	If the box **Never** is cleared (the default), the actions **Delayed On**, **Reboot**, and **Delayed Reboot** use this delay. In response to the action **Delayed On**, the outlet group waits the number of seconds configured for **Power On Delay** before it turns on. In response to the action **Reboot**, the outlet group turns off immediately, then waits the number of seconds configured for **Reboot Duration** and for **Power On Delay** before it turns on. In response to the action **Delayed Reboot**, the outlet group turns off after the number of seconds configured for **Power Off Delay**. The outlet group then waits the number of seconds configured for **Reboot Duration** and for **Power On Delay** before it turns on. If the box **Never** is check-marked, all outlets remain off when the UPS turns on, except when you use the **Immediate On** action.
Power Off Delay	The actions **Delayed Off** and **Delayed Reboot** use this delay. In response to the action **Delayed Off**, the outlet group waits the number of seconds configured for **Power Off Delay** before it turns off. In response to the action **Delayed Reboot**, the outlet group turns off after the number of seconds configured for **Power Off Delay**. The outlet group then waits the number of seconds configured for **Reboot Duration** and for **Power On Delay** before it turns on.

Delay	Definition
Reboot Duration	The actions **Reboot** and **Delayed Reboot** use this delay. In response to the action **Reboot**, the outlet group turns off immediately, then waits the number of seconds configured for **Reboot Duration** and for **Power On Delay** before it turns on. In response to the action **Delayed Reboot**, the outlet group turns off after the number of seconds configured for **Power Off Delay**. The outlet group then waits the number of seconds configured for **Reboot Duration** and for **Power On Delay** before it turns on.

General Settings (Outlet Groups)

Setting	Definition
Name	Defines a name for the outlet group. Use a name that describes the device or devices powered by the outlet group. The name is displayed with the outlet group number wherever the Web or control console interfaces display that number.
Link (URL) (Web interface only)	For each outlet group, defines a hyperlink that can be used from anywhere in the Web interface where the outlet group name is displayed. The default for each link is **http://www.apc.com**. You must use **http://** or **https://** when redefining any of the links. For example: • **https://www.*mysite*.com** • **http://www.apc.com**

Automatic Load Shedding for Outlet Groups (Web interface only)

Use the check-boxes provided to enable or disable the following settings for each outlet group, and configure a value for each setting that you enable. Use these settings to provide automatic, sequenced, load-shedding when a problem occurs with input voltage or battery capacity and to provide automatic sequenced start-up of outlet groups when the problem is resolved.

Note

These settings are disabled by default.

Type	Setting	Definition
Group Off Settings	Turn off when a power failure is longer than *n* seconds	Turn off the outlet group after input power fails for longer than the number of seconds you specify.
	Turn off when a power failure and battery capacity is less than *n*%	Turn off the outlet group when input power fails and battery capacity drops below the percentage you specify.
	Turn off when the UPS percent load is greater than *n*%	Turn off the outlet group when the output drawn from the UPS exceeds the percentage of UPS output overload that you specify.
Group On Settings	Turn on when the UPS returns from a power failure after the duration of *n* seconds	After the UPS switches from battery power to input power, wait the number of seconds you specify before the outlet group turns on.
	Turn on when the UPS returns from a power failure after battery capacity is greater than *n*%	Turn on the outlet group after input power to the UPS is restored and UPS battery capacity reaches the percentage of full capacity that you specify.

Module Status (Symmetra UPS or Symmetra PX UPS)

Menu options

Symmetra UPS models have a **Module Status** option in the Web interface that provides status information about the modules used at that UPS.

Symmetra UPS and Symmetra PX UPS models have the following options in the UPS menu of the control console:

- **Module Diagnostics & Information** provides module status.
- **Raw Status Data** provides diagnostic information about the modules. APC engineers and customer support technicians use these data to troubleshoot hardware problems.

Module status

Module status is reported for the following modules:

- The Intelligence Module
- The Redundant Intelligence Module
- The Power Modules
- The Battery in the Main Frame
- Any External Battery Frame
- Communication Bus (Symmetra PX UPS only)

For information about how to access a list of the UPS events, including the module-related, Symmetra status events, see "Event List" page.

PowerChute (UPS PowerChute Network Shutdown)

Overview

The **PowerChute** option of the UPS menu in the Web interface allows you to use the APC PowerChute Network Shutdown utility to shut down as many as 50 servers on your network that are using any client version of PowerChute Network Shutdown.

See also

For more information about PowerChute Network Shutdown, see the PowerChute Network Shutdown *Installation Guide* (Install.htm) and the PowerChute Network Shutdown *Release Notes* (Relnotes.htm), provided in the**.\pcns** directory on the APC Network Management Card *utility* CD. Also, see the three flow diagrams provided in the CD's **.\trouble** directory: **PCNS Shutdown Behavior.pdf**, **PCNS Low-Battery Shutdown Behavior.pdf**, and **PCNS Maximum Shutdown Time Negotiation.pdf**.

PowerChute Network Shutdown Parameters

Parameter	Definition
Maximum Shutdown Time	Defines the maximum time that the UPS at a PowerChute Network Shutdown client waits before it shuts down in response to a graceful turn-off command. **NOTE:** For information about this shutdown delay is determined, see Maximum-Shutdown-Time negotiation.
Shutdown Behavior	Defines how the UPS turns off after the PowerChute Network Shutdown clients finish shutting down their computer systems.
Add Client IP Address	Allows you to add as many as 50 PowerChute Network Shutdown clients to the list **Configured Client IP Addresses**. **NOTE:** When you install a PowerChute Network Shutdown client on your network, it is added to the list automatically.
Configured Client IP Addresses	Allows you to view the list of PowerChute Network Shutdown clients, and remove PowerChute Network Shutdown clients from the list. **NOTE:** When you uninstall a PowerChute Network Shutdown client, it is removed from the list automatically.

Maximum-Shutdown-Time negotiation

The **Maximum Shutdown Time** setting provides the delay needed to make sure that a server has enough time to shut down safely when the Management Card or PowerChute Network Shutdown client initiates a graceful shutdown at that server.

For information about the **Turn UPS Off Gracefully**, **Reboot UPS Gracefully**, and **Put UPS To Sleep Gracefully** options that use this delay for UPSs and Synchronized Control Groups, see Control.

The time reported by the **Maximum Shutdown Time** setting represents the maximum delay needed by at least one of the servers listed in the **Configured Client IP Addresses** list. This time is determined by a negotiation process that is initiated when any of the following occurs:

- The Management Card turns on (a **System: Coldstart** event)
- The Management Card is reset (a **System: Warmstart** event)
- You select **Force negotiation** from the **Maximum Shutdown Time** setting's drop-down menu, and click **Apply**

During the negotiation process, which can take up to 10 minutes, each server listed in **Configured Client IP Addresses** is contacted to determine the shutdown delay needed by that server. The delay time defined by the **Maximum Shutdown Time** setting will be changed, if necessary, to the highest delay time reported by the servers.

For example:

- If **3 minutes** was the result of the last negotiation process, and a new server that requires a 4-minute shutdown delay has been added to the **Configured Client IP Addresses** list, **4 minutes** will be the new **Maximum Shutdown Time**.
- If none of the servers needs more than a 2-minute delay, **2 minutes** will be the **Maximum Shutdown Time** setting.

Note

At the end of the negotiation process. two minutes time period is added to the calculated total for **Maximum Shutdown Time** to allow for any unusual delays that might occur in notifying servers to shut down.

See also

For a flowchart of the negotiation process, see the **PCNS Maximum Shutdown Time Negotiation.pdf** file provided in the **.\trouble** directory on the APC Network Management Card *utility* CD. The **.\trouble** directory also has two other flowchart presentations about PowerChute Network Shutdown: **PCNS Shutdown Behavior.pdf** and **PCNS Low-Battery Shutdown Behavior.pdf**.

Scheduling UPS Shutdown (Web interface only)

Overview

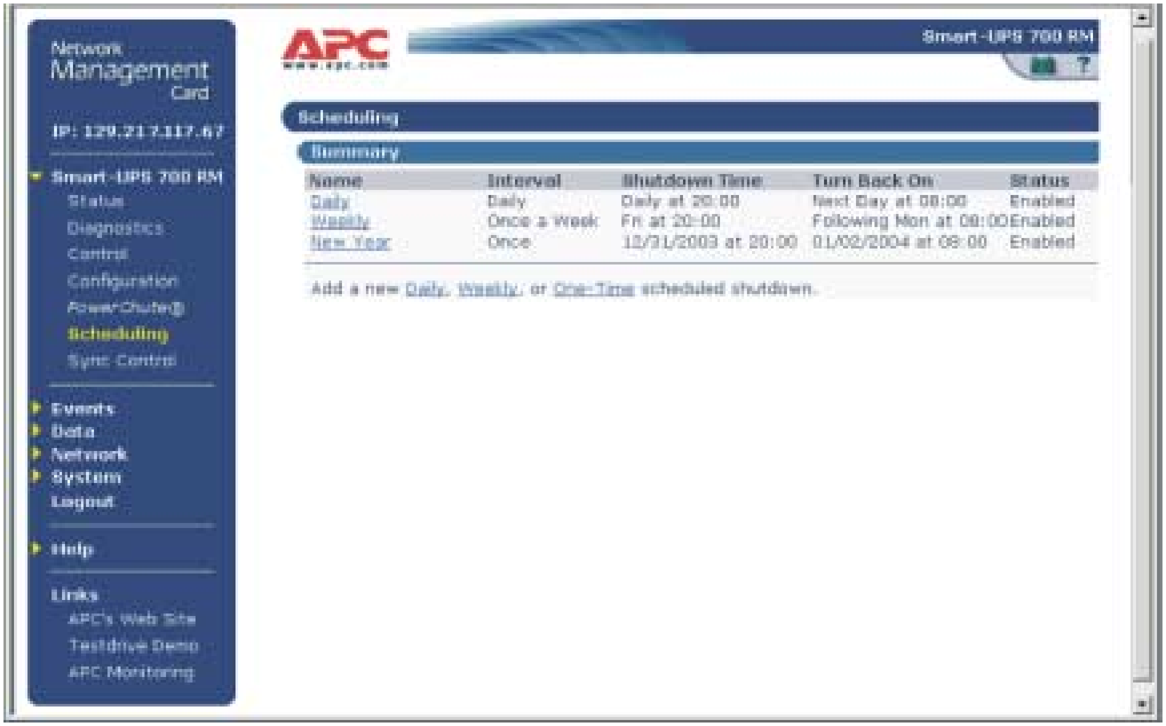
You can schedule shutdowns on a daily, weekly or one-time basis, and you can schedule them for a single UPS or for all UPSs in a Synchronized Control Group.

For more information about how to use this option, see the following sections:

- Examples
- How to schedule a shutdown
- How to schedule a synchronized shutdown
- How to edit, disable, or delete a shutdown

Examples

The following web page provides examples of **Daily**, **Weekly**, and **One-Time** shutdowns that were scheduled using the **Scheduling** option, which is available in the Web interface only.



Scheduling

Summary

Name	Interval	Shutdown Time	Turn Back On	Status
Daily	Daily	Daily at 20:00	Next Day at 08:00	Enabled
Weekly	Once a Week	Fri at 20:00	Following Mon at 08:00	Enabled
New Year	Once	12/31/2003 at 20:00	01/02/2004 at 08:00	Enabled

Add a new Daily, Weekly, or One-Time scheduled shutdown.

How to schedule a shutdown

Click the **Daily**, **Weekly**, or **One-Time** option to choose the type of shutdown, and then use the following fields:

1. Use **Name of Scheduled Shutdown** to define a name for the shutdown.
2. Use **Shutdown** to define when the shutdown will begin.
3. Use **Turn back on** to define whether the UPS will turn on at a specific day and time, **Never** (the UPS will be turned on manually), or **Immediately** (the UPS will turn on after a six-minute delay).
4. Select whether PowerChute servers will be warned before the shutdown begins.
5. Click **Apply**.

How to schedule a synchronized shutdown

To use the Network Management Card's Web interface to schedule shutdowns within a Synchronized Control Group, always schedule all shutdowns through the same member of the group.

The following guidelines apply to Synchronized Control Groups:

- All UPSs in a Synchronized Control Group must be the same model.
- Synchronized Control Groups are supported for most UPS models of the Smart-UPS and Symmetra UPS product lines. Any Smart-UPS or Symmetra UPS with a card slot that accepts a Network Management Card supports Synchronized Control Groups.
- In a Synchronized Control Group of Symmetra 3-phase UPSs, the shutdown mode setting must be either normal or secure for each UPS.
- For a scheduled UPS shutdown to occur, a network connection to the UPS must exist at the time at which the action is scheduled to occur.

Caution

SCHEDULED SHUTDOWNS THROUGH MORE THAN ONE GROUP MEMBER IS NOT A SUPPORTED CONFIGURATION AND MAY CAUSE UNPREDICTABLE RESULTS.

All scheduled shutdowns will be synchronized when the Network Management Card that initiates the shutdown is a member of a Synchronized Control Group and its status as a group member is enabled.

How to edit, disable, or delete a shutdown

Click a listed shutdown to display the “Daily Shutdown Detail” page. Use this page to do the following:

- View a summary of the shutdown, including information about the values for settings that can affect how the UPS shuts down and turns on again:
  - For information about **Maximum Shutdown Time**, a **PowerChute** option setting, see Maximum-Shutdown-Time negotiation
  - For information about **Shutdown Delay** and **Return Delay**, see Shutdown Parameters
- Change any shutdown parameter.
- Use **Status of Scheduled Shutdown** to enable, disable or delete the shutdown.

Sync Control

Overview

The **Sync Control** option of the UPS menu displays the status of each member of the Synchronized Control Group, if any, in which this Management Card is a member and the parameters necessary for this Management Card to be identified and operate as a member of the group.

The following guidelines apply to Synchronized Control Groups:

- All UPSs in a Synchronized Control Group must be the same model.
- Synchronized Control Groups are supported for most UPS models of the Smart-UPS and Symmetra UPS product lines. Any Smart-UPS or Symmetra UPS with a card slot that accepts a Network Management Card supports Synchronized Control Groups.
- In a Synchronized Control Group of Symmetra 3-phase UPSs, the shutdown mode setting must be either normal or secure for each UPS.

Sync Control Group Status

Item	Description
IP Address	The IP address of the group member
Input Status	The state of the group member's input power: **good** (acceptable) or **bad** (not acceptable)
Output Status	The status of the group members output power: **On** or **Off**

Configure Synchronized Control

Parameter	Description
Synchronized Group Membership	Determines whether this Synchronized Control Group member is an active member of its group. If you set this value to **Disabled** (the default value), the Management Card ignores all Synchronized Control Group commands, and its UPS functions as if it were not a member of any Synchronized Control Group.
Synchronized Control Group Number	The unique identifier of the Synchronized Control Group of which this Management Card's UPS is a member. This value must be a number from 1 through 65534. A UPS can be a member of only one Synchronized Control Group. All members of a Synchronized Control Group must have the same **Synchronized Control Group Number** and **Multicast IP Address**.
Power Synchronized Delay	The maximum time (120 seconds by default) that the initiating UPS of a synchronized sleep or reboot action will wait for other group members to regain input power when the initiating UPS is ready to turn on. • For a synchronized reboot, the initiating UPS waits up to this delay period for other group members to regain input power, then waits until its return battery capacity is reached, and then begins the **Return Delay**. The **Power Synchronized Delay** does not occur if all group members have input power immediately after they turn off for the reboot. • For a synchronized sleep command, after the configured sleep time expires, the initiating UPS waits up to this delay period for other group members to regain input power, and then begins the **Return Delay**. The **Power Synchronized Delay** does not occur if all group members have input power after the sleep time expires.
Return Battery Capacity Offset	An amount of battery capacity, as a percentage, that is configured individually for each member of the Synchronized Control Group. This offset percentage allows you to set a different and lower **Return Battery Capacity** for each group member for use during synchronized actions only. To determine the **Return Battery Capacity** that will be required of each participating group member during a synchronized **Turn UPS On**, **Reboot UPS**, **Reboot UPS Gracefully**, **Sleep**, or **Sleep Gracefully** action, this offset percentage is subtracted from the **Return Battery Capacity** of the UPS that initiates the action.

Parameter	Description
Multicast IP Address	The IP address used by members of a Synchronized Control Group to communicate with each other. This address must be within the range of 224.0.0.3 to 224.0.0.254. All members of the Synchronized Control Group must have the same group number and multicast IP address.

Environment Menu

Introduction

Overview

Use the **Environment** menu in the Web interface or control console to manage an external environmental monitor or the Integrated Environmental Monitor of an AP9618 or AP9619 Network Management Card. (In the control console, the **Environment** menu is an option of the **Device Manager** menu.)

- When you select the **Environment** option in an AP9617 Network Management Card's control console, you access the menu options used to manage an external environmental monitoring device.
- When you select the **Environment** option in an AP9618 Network Management Card's control console, two options may be available:

```
1- Integrated Environmental Monitor Settings
2- External Environmental Monitor Settings
```

Environment menu options

Two basic types of options are available:

- Status Options
- Settings Options

Note

Each of the control console's **Environmental Monitor Settings** menus has an **About Environmental Monitor** option that accesses firmware information for these environmental monitors; the Web interface provides this firmware information in the "Environmental Monitor Status" page.

Status Options

Overview

The “Summary Page” of the Web interface displays basic status information about the Integrated Environmental Monitor’s output relay at an AP9618 or AP9619 Network Management Card and about the thresholds and contacts of the Integrated Environmental Monitor or of an external environmental monitor.

Use the **Status** option in the **Environment** menu to access detailed status about these environmental monitor components, including how the current humidity and temperature readings relate to their high and low thresholds.

The Web interface uses icons to identify faults that exist at an environmental monitor. For information about these status icons, see Quick status tab.

In the control console, basic status information is displayed above the **Control Console** and **Environmental Monitor Settings** menus. Use **Threshold and Contact Details** (in the **External Environmental Monitor Settings** menu) and **Detailed Status** (in the **Integrated Environmental Monitor Settings** menu) for detailed status of the environmental monitor components.

Probe status

The Web interface uses Temperature and Humidity graphs to identify whether the reported value exceeds a low (blue) or high (red) threshold for each of the identified probes:

- Up to two probes at an AP9617 Network Management Card
- Up to three probes at an AP9618 or AP9619, Network Management Card with the Integrated Environmental Monitor probe listed last

In the control console, the status options in the **Environmental Monitor Settings** menus report the high and low thresholds for the specific environmental monitor's probes and any violations of those thresholds.

Contact status

The Web interface reports the current state (**Disabled**, **No Fault**, or **Fault Present**) for each identified input contact:

- Up to four contacts for an external environmental monitor
- Two contacts for the Integrated Environmental Monitor at an AP9618 or AP9619 Network Management Card.

In the control console, the status options in the **Environmental Monitor Settings** menus reports the current fault condition for each of the specific environmental monitor's contacts.

Output relay status (AP9618 or AP9619)

The Web interface reports the current state of the Integrated Environmental Monitor's output relay at an AP9618 or AP9619 Network Management Card.

In the control console, the **Output Relay** option in the **Integrated Environmental Monitor** menu reports the current condition.

Settings Options

Probe settings

In the Web interface, use the **Probes** option in the **Environment** menu to access the following fields:

- **Setting** fields that define a name (16-character maximum) and high and low temperature and humidity thresholds, for each probe.
- **Event Generation** fields that enable or disable the generation of an event when a selected threshold violation occurs.

In the control console, use the **Probe Settings** option in the **Environmental Monitor Settings** menus to define the probe name, temperature and humidity thresholds, and event generation settings.

Contact settings

In the Web interface, use the **Input Contacts** option in the **Environment** menu to access the following fields:

- **Name** fields to define the name for each contact alarm (16-character maximum).
- **Event Generation** fields to enable or disable each alarm.

In the control console, use the **Contact Settings** options in the **Environmental Monitor Settings** menu to access these settings.

Output relay settings (AP9618 or AP9619)

To access the following settings:

- In the Web interface, use the **Output Relay** option in the **Environment** menu.
- In the control console, use the **Output Relay Settings** option in the **Integrated Environmental Monitor** menu.

Setting	**Definition**
Output Relay (Web interface) Relay Name (control console	Defines a description of the output relay's purpose (16-character maximum).
Switch When (Web interface Switch Relay When (control console)	Selects the event that will activate the output relay (or disables the action).
Delay (Web interface) Switch to Relay Delay (control console)	Defines how long in seconds the event that is selected to activate the output relay must be present before the output relay is activated.
Hold (Web Interface) Relay Hold Time (control console)	Defines the minimum number of seconds that the output relay will remain activated after its activating event occurs.

Event-Related Menus

Introduction

Overview

Use the options of the **Events** menu to do the following tasks:

- Access the Event Log.
- Define the actions to be taken when an event occurs, based on the severity level of that event. (You must use the Web interface to define which events will use which actions.)
  - Event logging
  - Syslog messages
  - SNMP trap notification
  - E-mail notification

  To define which events will use which actions, see Event Log and How to Configure Individual Events.

- Define up to four SNMP trap receivers, by NMS-specific IP address or domain name, for event notifications by SNMP traps.
- Define up to four recipients for event notifications by e-mail.

Menu options

To access the event-related options:

- In the Web interface, use the **Events** menu.
- In the control console:
  - Use the **Email** option in the **Network** menu to define the SMTP server and e-mail recipients

- Use the **SNMP** option in the **Network** menu to define the SNMP trap receivers
- Use CTRL-L to access the event log from any menu

For information about event-related settings and about the e-mail feature, see the following descriptions:

- Event Log
- Event Actions (Web Interface Only)
- Event Recipients
- E-mail Feature
- How to Configure Individual Events

Event Log

Overview

The Management Card supports event logging for all UPS application firmware modules. You can record and view UPS, Environment (environmental monitor), and System (Management Card) events.

Use any of the following to view the Event Log:

- Web interface
- Control console
- FTP
- SCP

Logged events

By default, the following events are logged:

- Any event that causes an SNMP trap, except for SNMP authentication failures.
- The Management Card's abnormal internal system events.

To disable the logging of events based on their assigned severity level, use the **Actions** option in the Web interface's **Events** menu.

See Event Actions (Web Interface Only).

Even if you disable the Event Log for all severity levels, some System (Management Card) events will still be logged because some of those events have no severity level.

See "Event List" page to access a list of all configurable events (UPS, Management Card, and Environment) that indicates which events and how many events have been configured individually.

The Event Log will log a graceful shutdown of the UPS, even when that shutdown was not initiated by the Management Card

- A graceful shutdown from Serial Port 1 typically indicates that PowerChute performed the shutdown
- A graceful shutdown from Serial Port 0 typically indicates that a management peripheral, such as the Out-of-Band Management Card, initiated the shutdown.

Web interface

The **Log** option in the **Events** menu accesses the event log, which displays all of the events that have been recorded since the log was last deleted, in reverse chronological order. The **Delete Log** button clears all events from the log.

Control console

In the control console, press CTRL-L to display all the events that have been recorded since the log was last deleted, in reverse chronological order. Use the SPACE BAR to scroll through the recorded events.

While viewing the log, type `d` and press ENTER to clear all events from the log.

Note

Deleted events cannot be retrieved.

How to use FTP or SCP to retrieve log files

If you are an Administrator or Device Manager, you can use FTP or SCP to retrieve a tab-delineated event log file (*event.txt*) or data log file (*data.txt*) that you can import into a spreadsheet application.

- The file reports all of the events or data recorded since the log was last deleted.
- The file includes information that the event log or data log does not display.
  - The version of the file format (first field)
  - The date and time the file was retrieved
  - The **Name**, **Contact**, and **Location** values and IP address of the Management Card
  - The unique **Event Code** for each recorded event (*event.txt* file only)

Note

The Management Card uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits of the year.

If you are using the encryption-based security protocols for your system, use Secure CoPy (SCP) to retrieve the log file. (You should have FTP disabled.)

If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.

See Security for information on the available protocols and methods for setting up the type of security appropriate for your needs.

To use SCP to retrieve the files. To use SCP to retrieve the *event.txt* file, use the following command:

```
scp username@hostname_or_ip_address:event.txt ./event.txt
```

To use SCP to retrieve the *data.txt* file, use the following command:

```
scp username@hostname_or_ip_address:data.txt ./data.txt
```

To use FTP to retrieve the files. To use FTP to retrieve the *event.txt* or *data.txt* file:

1. At a command prompt, type `ftp` and the Management Card's IP address, and press ENTER.

   If the **Port** setting for **FTP Server** in the **Network** menu has changed from its default value (**21**), you must use the non-default value in the FTP command. For Windows FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

   ```
   ftp>open ip_address port_number
   ```

   To use non-default port values to enhance security, see Port assignments.

2. Use the case-sensitive **User Name** and **Password** for either an Administrator or a Device Manager user to log on.
   - For Administrator, **apc** is the default for **User Name** and **Password**.
   - For Device Manager, **device** is the default for **User Name**, and **apc** is the default for **Password**.
3. Use the **get** command to transmit the text-version of the event log or data log to your local drive.

   ```
   ftp>get event.txt
   ```

   or

   ```
   ftp>get data.txt
   ```
4. You can use the **del** command to clear the contents of the event log or data log.

   ```
   ftp>del event.txt
   ```

   or

   ```
   ftp>del data.txt
   ```

   You will not be asked to confirm the deletion.
   - If you clear the data log, the event log records a deleted-log event.
   - If you clear the event log, a new *event.txt* file is created to record the deleted-log event.
5. Type `quit` at the `ftp>` prompt to exit from FTP.

Event Actions (Web Interface Only)

Overview

Use the **Actions** option in the **Events** menu to do the following:

- Select which actions will occur for events that have a severity level:
  - **Event Log** selects which severity levels cause an event to be logged.

    See Event Log action.

  - **Syslog** selects which severity levels cause messages to be sent to Syslog servers to log events.

    See Syslog action.

  - **SNMP Traps** selects which severity levels generate SNMP traps, and which trap receivers are notified for events of each severity level.

    See SNMP Traps action.

  - **Email** selects which severity levels cause e-mail notifications and which e-mail recipients receive e-mail for events of each severity level

    See Email action.

  - **Paging** selects which severity levels initiate paging and which paging recipients are paged for events of each severity level.

    See Paging action.

- Click **Details** for a complete list of the Management Card (System), UPS, and environmental monitor (Environment) events that can occur, and then edit the actions that will occur for an individual event. Click **Hide Details** to return to the **Actions** option.

See How to Configure Individual Events.

Severity levels

Except for some System (Management Card) events that do not have a severity level, events are assigned a default severity level.

- **Informational**: Indicates an event that requires no action, such as a notification of a return from an abnormal condition.
- **Warning**: Indicates an event that may need to be addressed if the condition continues, but which does not require immediate attention.
- **Severe**: Indicates an event that requires immediate attention.
  - Unless resolved, severe UPS and Management Card events can cause incorrect operation of the UPS or its supported equipment, or can result in the loss of UPS protection during a power failure.
  - Severe environmental monitoring device events warn of abnormal environmental conditions or possible security violations.

Event Log action

To stop logging events that have a severity level, disable the **Event Log** action. System (Management Card) events that have no severity level will still be logged. By default, all events are logged, even events that have no severity level.

For more information about the log, see Event Log.

Syslog action

By default, the **Syslog** action is enabled for all events that have a severity level. However, before you can use this feature to send Syslog messages when events occur, you must configure it.

See Syslog.

SNMP Traps action

By default, the **SNMP Traps** action is enabled for all events that have a severity level. However, before you can use SNMP traps for event notification, you must identify the NMSs (by their IP addresses or domain names) that will receive the traps.

To define up to four NMSs as trap receivers, see Event Recipients.

Email action

By default, the **Email** action is enabled for all events that have a severity level. However, before you can use e-mail for event notification, you must define the e-mail recipients.

See E-mail Feature.

Paging action

By default, the **Paging** action is enabled for all severe events. However, before you can use paging for event notification, you must define the paging recipients.

To define up to four paging recipients, see Configure Paging Recipients.

Event Recipients

Overview

Use the Web interface or control console to define up to four trap receivers, four e-mail addresses, and four paging recipients to be used when an event occurs that has SNMP, e-mail, or paging enabled, as described in Event Actions (Web Interface Only).

To identify the servers that will receive Syslog messages, see Syslog.

Trap Receivers

To define the **Trap Receiver** settings that determine which NMSs receive traps:

- In the Web interface, use the **Recipients** option in the **Events** menu.
- In the control console, use the **SNMP** option in the **Network** menu.

Item	Definition
Community Name	The password (maximum of 15 characters) used when traps are sent to the NMS identified by the **Receiver NMS IP** setting.
Receiver NMS IP/ Domain Name	The IP address or domain name of the NMS that will receive traps. **0.0.0.0** (the default value) causes traps not to be sent to any NMS.
Generation (Web Interface) Trap Generation (control console)	Enables (by default) or disables the sending of any traps to the NMS identified by the **Receiver NMS IP/Domain Name** setting.
Authentication Traps	Enables or disables the sending of authentication traps to the NMS identified by the **Receiver NMS IP/Domain Name** setting.

Email options

See E-mail Feature.

E-mail Feature

Overview

Use the Simple Mail Transfer Protocol (SMTP) to send e-mail to up to four recipients when an event occurs.

To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and secondary Domain Name Service (DNS) servers

  See DNS servers.

- The DNS name of the **SMTP Server** and the **From Address** settings for SMTP

  See SMTP settings.

- The e-mail addresses for a maximum of four recipients

  See Email Recipients.

Note

You can use the **To Address** setting of the **Email Recipients** option to send e-mail to a text-based pager.

DNS servers

The Management Card cannot send any e-mail messages unless at least the IP address of the primary DNS server is defined.

See DNS.

The Management Card will wait a maximum of 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the Management Card does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers that are on the same segment as the Management Card, or on a nearby segment (but not across a wide-area network (WAN).

After you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to look up the IP address for computer.

SMTP settings

Use the **Email** option in the **Network** menu to define the following settings:

Setting	Description
SMTP Server	The IP address (or if DNS is configured, The DNS name) of the SMTP server. **NOTE:** This definition is required only when the **SMTP Server** option is set to **Local**. See Email Recipients.
From Address	The contents of the **From** field in the format *user@domain*.com (if an IP address is specified as **SMTP Server**) or *user@* [*IP_address*] (if DNS is configured and the DNS name is specified as **SMTP Server**) in the e-mail messages sent by the Management Card. **NOTE:** The SMTP server's configuration may require that you use a valid user account on the server for this setting. See the server's documentation for more information.

Email Recipients

In the Web interface, use the **Recipients** option in the **Events** menu or the **Configure the Email recipients** link in the “Email Configuration” page to identify up to four e-mail recipients. Use the **Email Test** option to send a test message to a configured recipient.

In the control console, use the **Email** option in the **Network** Menu, to access the e-mail recipient settings.

Setting	Description
To Address†	Defines the user and domain names of the recipient. To use e-mail for paging, use the e-mail address for that recipient's pager gateway account (for example, `myacct100@skytel.com`). The pager gateway will generate the page. **NOTE:** The recipient's pager must be able to use text-based messaging.
Use SMTP Server	Selects one of the following methods for routing e-mail: • Through the Management Card's SMTP server (the recommended option, **Local**. This option ensures that the e-mail is sent before the Management Card's 20-second time-out, and, if necessary, is retried several times. Also do one of the following: •Enable forwarding at the Management Card's SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Always check with the administrator of your SMTP server before changing its configuration to allow forwarding. •Set up a special e-mail account for the Management Card to forward e-mail to an external mail account. • Directly to the recipient's SMTP server (the **Recipient's** option). On a busy remote SMTP server, the time-out may prevent some e-mail from being sent, and with this option the Management Card tries to send the e-mail only once. When the recipient uses the Management Card's SMTP server, this setting has no affect.
Generation	Enables (by default) or disables sending e-mail to the recipient.

† You can bypass the DNS lookup of the mail server's IP address by using the IP address in brackets instead of the e-mail domain name. For example, use jsmith@[xxx,xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.

Setting	Description
Format	Selects the format used for e-mail messages: **Short**: Identifies only the event that occurred. For example: UPS: Communications Established **Long**: Includes information about the Management Card and the UPS, as well as the event. For example: Name : Test Lab Location : Building 3 Contact : Don Adams http://139.225.6.133 Serial # : Wa12 UPS Ser # : XS9849007541 Date: 03/12/2004 Time: 16:09:48 Code: 0x0102 Severe - UPS: Communications Lost

† You can bypass the DNS lookup of the mail server's IP address by using the IP address in brackets instead of the e-mail domain name. For example, use jsmith@[xxx,xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.

How to Configure Individual Events

"Event List" page

The **Actions** option in the **Events** menu opens the "Event Actions Configuration" page. Use the **Details** button on that page for a complete list of the Management Card (System), UPS, and environmental monitor (Environment) events that can be reported by your Management Card.

On the "Event List" page, an asterisk at the beginning of an event description indicates that the event has been configured individually and is no longer set to its default configuration. A message at the bottom of the page indicates how many events have been configured.

Each event is identified by its unique code, its description, and its assigned severity level, as shown in the following examples.

For information about severity levels and how they define the actions associated with events, see Event Actions (Web Interface Only).

Code	Description	Severity
0x0008	System: Password changed.	Informational
0x0109	UPS: Switched to battery backup power.	Warning
0x030F	Environment: High humidity threshold violation on probe 1.	Severe

“Detailed Event Action Configuration” page

Each event code on the “Event List” page is a link to a page that allows you to do the following:

- Change the selected event’s severity level
- Enable or disable whether the event uses the Event Log, Syslog messages, SNMP traps, paging, or e-mail notifications
- Reset the event to its default configuration

Log Option

Use this option to access a log that stores information about the UPS, the power input to that UPS, and the ambient temperature and relative humidity measured by an environmental monitor’s probes.

Use the **Data** menu’s **Configuration** option to define how frequently data is sampled and stored in the data log. Each entry is listed by the date and time the data was recorded, and provides the data in a column format.

The data recorded depends on the UPS model.

See Configuration Option.

See also

For descriptions of the recorded data that is specific to your UPS, see the online help in your Management Card’s Web interface.

To retrieve the data log as a text file, see How to use FTP or SCP to retrieve log files.

Configuration Option

Use this option to access the “Data Log Configuration” page. which reports how much data can be stored in the data log. If you change the **Log Interval** setting, which defines how often data will be sampled and recorded in the data log, the report updates based on the new setting.

The minimum interval is **60** seconds; the maximum interval is **8** hours, **10** minutes, **15** seconds.

Boot Mode

Introduction

Overview

In addition to using a BOOTP server or manual settings, the Network Management Card can use a dynamic host configuration protocol (DHCP) server to provide the settings the Management Card needs to operate on a TCP/IP network.

To use a DHCP server to provide the Management Card's network settings, use **Boot mode**, a **TCP/IP** option in the **Network** menu. **Boot mode** must be set to either **DHCP & BOOTP**, its default setting, or **DHCP only**.

See also

For information on DHCP and DHCP options, see RFC2131 and RFC2132.

DHCP & BOOTP boot process

When **Boot mode** is set to its default **DHCP & BOOTP** setting, the following occurs when the Management Card is turned on or reset:

1. The Management Card makes up to five requests for its network assignment from any BOOTP server. If a valid BOOTP response is received, the Management Card starts the network services and sets **Boot mode** to **BOOTP Only**.
2. If the Management Card fails to receive a valid BOOTP response after five BOOTP requests, the Management Card makes up to five requests for its network assignment from any DHCP server. If a valid DHCP response is received, the Management Card starts the network services and sets **Boot mode** to **DHCP Only**.

   Note: To configure the Management Card so that it always uses the **DHCP & BOOTP** setting for **Boot mode**, enable the option **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**, which is disabled by default.

   See Management Card settings.

3. If the Management Card fails to receive a valid DHCP response after five DHCP requests, it repeats sending BOOTP and DHCP requests until it receives a valid network assignment: first it sends a BOOTP request every 32 seconds for 12 minutes, then it sends one DHCP request with a time-out of 64 seconds, and so forth.

Note

If a DHCP server responds with an invalid offer (for example, the offer does not contain the APC Cookie), the Management Card accepts the lease from that server on the last request of the sequence and then immediately releases that lease. This prevents the DHCP server from reserving the IP Address associated with its invalid offer.

For more information on what a valid response requires, see DHCP response options.

For more information on what a valid response requires, see DHCP response options.

DHCP Configuration Settings

Management Card settings

Use the **TCP/IP** option in the **Network** menu of either the Web interface or the control console to configure the network settings of the Management Card.

- The **Port Speed**, **Host Name**, and **Domain Name** settings are available for any **Boot mode** selection
- The **Vendor Class**, **Client ID**, and **User Class** settings are available for any **Boot mode** selection except **Manual**.

See Advanced settings.

When **Boot mode** is set to **DHCP & BOOTP**, two options are available:

- **After IP Assignment** in the control console (or **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** in the Web interface): By default, this option switches **Boot mode** to the selection based on the server that provided the TCP/IP settings (**DHCP Only** or **BOOTP Only**).
- **DHCP Cookie Is** in the control console (or **Require vendor specific cookie to accept DHCP Address** in the Web interface): By default, this option requires that the DHCP responses include the APC cookie in order to be valid.

For more information about the APC cookie, see DHCP response options.

When **Boot mode** is set to **DHCP Only**. two options are available:

- **DHCP Cookie Is** in the control console (or **Require vendor specific cookie to accept DHCP Address** in the Web interface): By default, this option requires that the DHCP responses include the APC cookie in order to be valid.
- **Retry Then Stop** in the control console (**Maximum # of Retries** in the Web interface), This option sets the number of times the Management Card will repeat the DHCP request if it does not receive a valid response. The default setting (**0** in the Web interface, **None** in the control console), requires that the Management Card continuously send out DHCP requests until a valid DHCP response is received.

DHCP response options

Each valid DHCP response contains options that provide the TCP/IP settings a Management Card needs to operate on a network and other information that affects the Management Card's operation.

A Management Card uses the Vendor Specific Information option (option 43) in a DHCP response to determine whether the DHCP response is valid.

Vendor Specific Information (option 43). The Vendor Specific Information option contains up to two APC-specific options encapsulated in a TAG/LEN/DATA format: the APC Cookie and the Boot Mode Transition.

APC Cookie. Tag 1, Len 4, Data "1APC"

Option 43 communicates to the Management Card that a DHCP server has been configured to service APC devices. By default, the APC Cookie must be present in this DHCP response option before a Management Card can accept the lease.

To disable the requirement of an APC cookie, see Management Card settings for information on the **DHCP Cookie Is** setting.

Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie:

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43
```

Boot Mode Transition. Tag 2, Len 1, Data 1/2

This option 43 setting enables or disables the **After IP Assignment** option which, by default, causes the **Boot mode** option to base its setting on the server that provided the network assignment values (**DHCP Only** or **BOOTP Only**):

- A data value of 1 disables the **After IP Assignment** option. The **Boot mode** option remains as **DHCP & BOOTP** after network values are assigned successfully. Whenever the Management Card reboots, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.

  See DHCP & BOOTP boot process.

- A data value of 2 enables the **After IP Assignment** option. The **Boot mode** option switches to **DHCP Only** when the Management Card accepts the DHCP response. Whenever the Management Card reboots, it will request its network assignment from a DHCP server, only.

  For more information about the **After IP Assignment** option, see Management Card settings.

Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie and the disable Boot Mode Transition setting:

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43 0x02 0x01 0x01
```

TCP/IP options. A Management Card uses the following options within a valid DHCP response to define its TCP/IP settings:

- **IP Address** (from the **yiaddr** field of the DHCP response): The IP address that the DHCP server is leasing to the Management Card**.**
- **Subnet Mask** (option 1): The Subnet Mask value which the Management Card needs to operate on the network.
- **Default Gateway** (option 3): The default gateway address, which the Management Card needs to operate on the network.
- **Address Lease Time** (option 51): The time duration for the lease associated with the identified **IP Address.**
- **Renewal Time, T1** (option 58): The time that the Management Card must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): The time that the Management Card must wait after an IP address lease is assigned before it can seek to rebind that lease.

Other options. A Management Card uses the following options within a valid DHCP response to define NTP, DNS, hostname and domain name settings:

- **NTP Server, Primary and Secondary** (option 42): Up to two NTP servers that can be used by the Management Card.
- **NTP Time Offset** (option 2): The offset of the Management Card's subnet, in seconds, from Coordinated Universal Time (UTC), formerly Greenwich Mean Time (GMT).
- **DNS Server, Primary and Secondary** (option 6):Up to two DNS servers that can be used by the Management Card.
- **Host Name** (option 12): The host name to be used by the Management Card (32-character maximum length).
- **Domain Name** (option 15): The domain name to be used by the Management Card (64-character maximum length).

Security

Security Features

Planning and implementing security features

As a network device that passes information across the network, the Network Management Card is subject to the same exposure as other devices on the network.

Use the information in this section to plan and implement the security features appropriate for your environment.

Summary of access methods

Serial control console.

Security Access	Description
Access is by user name and password.	Always enabled.

Remote control console.

Security Access	Description
Available methods: • User name and password • Selectable server port • Server Enable/Disable • Secure SHell (SSH)	For high security, use SSH. • With Telnet, the user name and password are transmitted as plain text. • SSH disables Telnet and provides encrypted access to the control console interface to provide additional protection from attempts to intercept, forge, or alter data during data transmission.

SNMP.

Security Access	Description
Available methods: • Community Name • Domain Name • NMS IP filters • Agent Enable/Disable • 4 access communities with read/write/disable capability	The domain name restricts access only to the NMS as that location, and the NMS IP filters allow access only from designated IP addresses. • 162.245.12.1 allows only the NMS with that IP address to have access. • 162.245.12.255 allows access for any NMS on the 162.245.12 segment. • 162.245.255.255 allows access for any NMS on the 162.245 segment. • 162.255.255.255 allows access for any NMS on the 162 segment. • 0.0.0.0 or 255.255.255.255 allows access for any NMS.

File transfer protocols.

Security Access	Description
Available methods: • User name and password • Selectable server port • Server Enable/Disable • Secure CoPy (SCP)	With FTP, the user name and password are transmitted as plain text, and files are transfered without the protection of encryption. Using SCP instead of FTP encrypts the user name and password and the files being transferred, such as firmware updates, configuration files, log files, Secure Socket Layer (SSL) certificates, and Secure SHell (SSH) host keys. If you choose SCP as your file transfer protocol, enable SSH and disable FTP.

Web Server.

Security Access	Description
Available methods: • User name and password • Selectable server port • Server Enable/Disable • MD5 authentication • Secure Socket Layer (SSL) and Transport Layer Security (TLS)	In basic HTTP authentication mode, the user name and password are transmitted base-64 encoded (with no encryption). MD5 authentication mode uses a user name and password phrase. SSL and TLS are available on Web browsers supported for the Network Management Card and on most Web servers. The Web protocol Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) encrypts and decrypts page requests to the Web server and pages returned by the Web server to the user.

Changing default user names and passwords immediately

As soon as you complete the installation and initial configuration of the Management Card, immediately change the default user names and passwords. Configuring unique user names and passwords is essential to establish basic security for your system.

Port assignments

If a Telnet, FTP, SSH/SCP, or Web/SSL/TLS server uses a non-standard port, a user must specify the port when using the client interface, such as a Web browser. The non-standard port address becomes an extra “password,” hiding the server to provide an additional level of security. The TCP ports for which these servers listen are initially set at the standard “well known ports” for the protocols. To hide the interfaces, use any port numbers from 5000 to 32768.

User names, passwords, community names (SNMP)

All user names, passwords, and community names for SNMP are transferred over the network as plain text. A user who is capable of monitoring the network traffic can determine the user names and passwords required to log on to the accounts of the control console or Web interface of the Network Management Card. If your network requires the higher security of the encryption-based options available for the control console and Web interface, be sure to disable SNMP access or set its access to read-only. (Read-only access allows you to receive status information and to use SNMP traps.)

Authentication

Authentication vs. encryption

You can select to use security features for the Network Management Card that control access by providing basic authentication through user names, passwords, and IP addresses, without using encryption. These basic security features are sufficient for most environments in which sensitive data are not being transferred.

For a security method that provides additional authentication for the Web interface, but does not provide the higher security of encryption, use Message Digest 5 (MD5) Authentication.

See MD5 authentication (for the Web interface).

To ensure that data and communication between the Network Management Card and the client interfaces, such as the control console and the Web interface, cannot be intercepted, you can provide a greater level of security by using one or more of the following encryption-based methods:

- For the Web interface, use the Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols. You can also use these protocols in combination with MD5 authentication.
- To encrypt user names and passwords for control console access, use the Secure SHell (SSH) protocol.
- To encrypt user names, passwords, and data for the secure transfer of files, use the Secure CoPy (SCP) protocol.

For more information on these protocols for encryption-based security, see Secure SHell (SSH) and Secure CoPy (SCP) and Secure Socket Layer (SSL)/Transport Layer Security (TLS).

MD5 authentication (for the Web interface)

The Web interface option for MD5 authentication enables a higher level of access security than the basic HTTP authentication scheme. The MD5 scheme is similar to CHAP and PAP remote access protocols. Enabling MD5 implements the following security features:

- The Web server requests a user name and a password phrase (distinct from the password). The user name and password phrase are not transmitted over the network, as they are in basic authentication. Instead, a Java login applet combines the user name, password phrase, and a unique session challenge number to calculate an MD5 hash number. Only the hash number is returned to the server to verify that the user has the correct login information; MD5 authentication does not reveal the login information.
- In addition to the login authentication, each form post for configuration or control operations is authenticated with a unique challenge and hash response.
- After the authentication login, subsequent page access is restricted by IP addresses and a hidden session cookie. (You must have cookies enabled in your browser.) Pages are transmitted in their plain-text form, with no encryption.

If you use MD5 authentication for the Web interface, be sure to increase the security for other interfaces to the Management Card.

- **Control console:** Use SSH (which disables Telnet) for encrypted access.
- **File transfer:** Disable FTP, and instead use SCP, which encrypts user names, passwords, and files.
- **SNMP:** Disable SNMP or disable its write access. With read-only access, trap facilities remain available.

See also

For additional information on MD5 authentication, see RFC document #1321 at **http://www.ietf.org**, the Web site of the Internet Engineering Task Force. For CHAP, see RFC document #1994.

You can use MD5 and the encryption-based SSL/TSL security protocols together. See Secure Socket Layer (SSL)/ Transport Layer Security (TLS) for an example of the extra security benefits of using both.

Encryption

Secure SHell (SSH) and Secure CoPy (SCP)

The Secure SHell (SSH) protocol provides a secure mechanism to access computer consoles or *shells* remotely. The protocol authenticates the server (in this case, the Network Management Card) and encrypts all transmissions between the SSH client and the server.

- SSH is an alternative to Telnet, which does not provide encryption.
- SSH protects the username and password, the credentials for authentication, from being used by anyone intercepting network traffic.
- To authenticate the SSH server (the Network Management Card) to the SSH client, SSH uses a host key that is unique to the SSH server and that provides an identification that cannot be falsified. Therefore, an invalid server on the network cannot obtain a user name and password from a user by presenting itself as a valid server.

To create a host key, see Create an SSH Host Key.

- The Network Management Card supports versions 1 and 2 of SSH. The encryption mechanisms of the versions differ, and each version has advantages. Version 1 provides faster login to the Management Card, and version 2 provides improved protection from attempts to intercept, forge or change data that are transmitted.
- When you enable SSH, Telnet is automatically disabled.
- The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet.

For information on supported SSH client applications, see Telnet/SSH.

Secure CoPy (SCP) is a secure file transfer application that you can use instead of FTP. SCP uses the SSH protocol as the underlying transport protocol for encryption of user names, passwords, and files.

- When you enable and configure SSH, you automatically enable and configure SCP. No further configuration of SCP is needed.
- You must explicitly disable FTP. It is **not** disabled by enabling SSH.

Secure Socket Layer (SSL)/Transport Layer Security (TLS)

For secure Web communication, you enable Secure Socket Layer (SSL) and Transport Layer Security (TLS) by selecting HTTPS (SSL/TLS) as the protocol mode to use for access to the Web interface of the Network Management Card. Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) is a Web protocol that encrypts and decrypts page requests from the user and pages that are returned by the web server to the user. Originally developed by Netscape, it has become an internet standard supported by most Web browsers.

The Network Management Card supports SSL version 3.0 and TLS version 1.0. Most browsers let you select the version of SSL to enable.

When SSL is enabled, your browser displays the lock icon, usually at the bottom of the screen.

SSL uses a digital certificate to enable the browser to authenticate the server (in this case, the Network Management Card). The browser verifies the following:

- The format of the server certificate is correct.
- The server certificate’s expiration date and time has not passed.
- The DNS name or IP address specified when a user logs on matches the common name in the server certificate.
- The server certificate is signed by a trusted certifying authority.

Each major browser manufacturer distributes CA root certificates of the commercial Certificate Authorities in the certificate store (cache) of its browser so that it can compare the signature on the server certificate to the signature on a CA root certificate.

You can use the APC Security Wizard, provided on the APC Network Management Card *utility* CD, to create a certificate signing request to an external Certificate Authority, or if you do not want to use an existing Certificate Authority, you can create an APC root certificate to upload to a browser's certificate store (cache). You can also use the Wizard to create a server certificate to upload to the Management Card.

See Creating and Installing Digital Certificates for a summary of how these certificates are used.

To create certificates and certificate requests, see Create a Root Certificate & Server Certificates and Create a Server Certificate and Signing Request.

SSL also uses various algorithms and encryption ciphers to authenticate the server, encrypt data, and ensure the integrity of the data (i.e. that it has not been intercepted and sent by another server).

See CipherSuite to select which authentication and encryption algorithms to use.

You can use SSL/TLS and MD5 authentication together to provide the security benefits of both. MD5 authentication does not provide encryption, but its authentication methods can be a useful enhancement to the security provided by SSL/TLS.

Note

Web browsers cache (save) Web pages that you recently accessed and allow you to return to those pages without re-entering your user name and password. MD5 authentication, however, requires you to enter your user name and password even to access a cached Web page, e.g., when you use the **Back** button of Microsoft Internet Explorer. Therefore, if you are use the SSL and TLS protocols without also using MD5 authentication, always close your browser session before you leave your computer unattended.

Creating and Installing Digital Certificates

Purpose

For network communication that requires a higher level of security than password encryption, the Web interface of the Network Management Card supports the use of digital certificates with the Secure Socket Layer (SSL) protocol. Digital certificates can authenticate the Network Management Card (the server) to the Web browser (the SSL client).

The sections that follow summarize the three methods of creating, implementing, and using digital certificates. Read these sections to determine the most appropriate method for your system.

- Method 1: Use the Network Management Card's auto-generated default certificate.
- Method 2: Use the APC Security Wizard to create a CA certificate and a server certificate.
- Method 3: Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate.

Note

You can also use Method 3 if your company or agency operates its own Certificate Authority. Use the APC Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

Choosing a method for your system

Using the Secure Socket Layer (SSL) protocol, you can choose any of the following methods for using digital certificates.

Method 1: Use the Network Management Card's auto-generated default certificate. When you enable SSL, you must reboot the Management Card. During rebooting, if no server certificate exists on the Management Card, the Management Card generates a default server certificate that is self-signed but that you cannot configure.

This method has the following advantages and disadvantages:

- **Advantages:**
  - Before they are transmitted, the user name and password for Management Card access and all data to and from the Management Card are encrypted.
  - You can use this default server certificate to provide encryption-based security while you are setting up either of the other two digital certificate options, or you can continue to use it for the benefits of encryption that SSL provides.
- **Disadvantages:**
  - The Management Card takes up to 5 minutes to create this certificate, and the Web interface is not available during that time. (This delay occurs the first time you log on after you enable SSL.)
  - This method does not include the browser-based authentication provided by a CA certificate (a certificate signed by a Certificate Authority) as Methods 2 and 3 provide. There is no CA Certificate cached in the browser. Therefore, whenever you log on to the Management Card, the browser generates a security alert, indicating that a certificate signed by a trusted authority is not available and asking if you want to proceed.

- The default server certificate on the Management Card has the Management Card's serial number in place of a valid *common name* (the DNS name or the IP address of the Management Card). Therefore, although the Management Card can control access to its Web interface by user name, password, and account type (e.g., **Administrator**, **Device Manager**, or **Read Only User**), the browser cannot authenticate what Management Card is sending or receiving data.
- The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is only 768 bits. (The public key used in Methods 2 and 3 is 1024 bits, providing more complex encryption and consequently a higher level of security.)

Method 2: Use the APC Security Wizard to create a CA certificate and a server certificate. You use the APC Security Wizard to create two digital certificates:

- A *CA root certificate* (Certificate Authority root certificate) that the APC Security Wizard uses to sign all server certificates and which you then install into the certificate store (cache) of the browser of each user who needs access to the Management Card.
- A *server certificate* that you upload to the Management Card. When the APC Security Wizard creates a server certificate, it uses the CA root certificate to sign the server certificate.

The Web browser authenticates the Management Card sending or requesting data:

- To identify the Management Card, the browser uses the *common name* (IP address or DNS name of the Management Card) that was specified in the server certificate's *distinguished name* when the certificate was created.
- To confirm that the server certificate is signed by a “trusted” signing authority, the browser compares the signature of the server certificate with the signature in the root certificate cached in the browser. An expiration date confirms whether the server certificate is current.

This method has the following advantages and disadvantages.

- **Advantages:**
  - Before they are transmitted, the user name and password for Management Card access and all data to and from the Management Card are encrypted.
  - The length of the *public key* (RSA key) that is used for encryption when setting up an SSL session is 1024 bits, providing more complex encryption and consequently a higher level of security than

the public key used in Method 1. (This longer encryption key is also used in Method 3.)

- The server certificate that you upload to the Management Card enables SSL to authenticate that data are being received from and sent to the correct Management Card. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
- The root certificate that you install to the browser enables the browser to authenticate the Management Card's server certificate to provide additional protection from unauthorized access.

- **Disadvantage:**
  Because the certificates do not have the digital signature of a commercial Certificate Authority, you must load a root certificate individually into the certificate store (cache) of each user's browser. (Browser manufacturers already provide root certificates for commercial Certificate Authorities in the certificate store within the browser. See Method 3.)

Method 3: Use the APC Security Wizard to create a certificate-signing request to be signed by the root certificate of an external Certificate Authority and to create a server certificate. You use the APC Security Wizard to create a request (a **.csr** file) to send to a Certificate Authority. The Certificate Authority returns a signed certificate (a **.crt** file) based on information you submitted in your request. You then use the APC Security Wizard to create a server certificate (a **.p15** file) that includes the signature from the root certificate returned by the Certificate Authority. You upload the server certificate to the Management Card.

Note

You can also use Method 3 if your company or agency operates its own Certificate Authority, Use the APC Security Wizard in the same way, but use your own Certificate Authority in place of a commercial Certificate Authority.

This method has the following advantages and disadvantages.

- **Advantages:**
  - Before they are transmitted, the user name and password for Management Card access and all data to and from the Management Card are encrypted.
  - You have the benefit of authentication by a Certificate Authority that already has a signed root certificate in the certificate cache of the browser. (The CA certificates of commercial Certificate Authorities are distributed as part of the browser software, and a Certificate Authority of your own company or agency has probably already loaded its CA certificate to the browser store of each user's browser.) Therefore, you do not have to upload a root certificate to the browser of each user who needs access to the Management Card.
  - The length of the *public key* (RSA key) that is used for setting up an SSL session is 1024 bits, providing more complex encryption and

consequently a higher level of security than the public key used in Method 1 (This longer encryption key is also used in Method 2.)

 - The server certificate that you upload to the Management Card enables SSL to authenticate that data are being received from and sent to the correct Management Card. This provides an extra level of security beyond the encryption of the user name, password, and transmitted data.
 - The browser matches the digital signature on the server certificate that you uploaded to the Management Card with the signature on the CA root certificate that is already in the browser's certificate cache to provide additional protection from unauthorized access.

- **Disadvantages:**
  - Setup requires the extra step of requesting a signed root certificate from a Certificate Authority.
  - An external Certificate Authority may charge a fee for providing signed certificates.

Firewalls

Although some methods of authentication provide a higher level of security than others, complete protection from security breaches is almost impossible to achieve. Well-configured firewalls are an essential element in an overall security scheme.

Using the APC Security Wizard

Overview

Authentication

Authentication verifies the identity of a user or a network device (such as an APC Network Management Card). Passwords typically identify computer users. However, for transactions or communications requiring more stringent security methods on the Internet, the Network Management Card supports more secure methods of authentication.

- Secure Socket Layer (SSL), used for secure Web access, uses digital certificates for authentication. A digital *CA root* certificate is issued by a Certificate Authority (CA) as part of a public key infrastructure, and its digital signature must match the digital signature on a server certificate on the Management Card.
- Secure SHell (SSH), used for remote terminal access to the Management Card's control console, uses a public *host key* for authentication rather than a digital certificate.

How certificates are used. Most Web browsers, including all browsers supported by the Network Management Card, contain a set of CA root certificates from all of the commercial Certificate Authorities.

Authentication of the server (in this case, the Management Card) occurs each time a connection is made from the browser to the server. The browser checks to be sure that the server's certificate is signed by a Certificate Authority known to the browser. For this authentication to occur:

- Each Network Management Card with SSL enabled must have a server certificate on the Management Card itself.
- Any browser that is used to access the Management Card's Web interface must contain the CA root certificate that signed the server certificate.

If authentication fails, the browser prompts you on whether to continue despite the fact that it cannot authenticate the server.

If your network does not require the authentication provided by digital certificates, you can use the default certificate that the Management Card generates automatically. The default certificate's digital signature will not be recognized by browsers, but a default certificate enables you to use SSL for the encryption of transmitted user names, passwords, and data. (If you use the default certificate, the browser prompts you to agree to unauthenticated access before it logs you on to the Web interface of the Management Card.)

How SSH host keys are used. An SSH *host key* authenticates the identity of the server (the Network Management Card) each time an SSH client contacts the Management Card. Each Network Management Card with SSH enabled must have an SSH host key on the Management Card itself.

Files you create for SSL and SSH security

Use the APC Security Wizard to create the following components of an SSL and SSH security system:

- The server certificate for the Network Management Card, if you want the benefits of authentication that such a certificate provides.You can create either of the following types of server certificate:
  - A server certificate signed by a custom CA root certificate also created with the APC Security Wizard. Use this method if your company or agency does not have its own Certificate Authority and you do not want to use an external Certificate Authority to sign the server certificate.
  - A server certificate signed by an external Certificate Authority. This Certificate Authority can be one that is managed by your own company or agency or can be one of the commercial Certificate Authorities whose CA root certificates are distributed as part of a browser's software.
- A certificate signing request containing all the information required for a server certificate except the digital signature. You need this request if you are using an external Certificate Authority.
- A CA root certificate.
- An SSH host key that your SSH client program uses to authenticate the Management Card when you log on to the control console interface.

Note

All public keys for SSL certificates and all host keys for SSH that are created with the APC Security Wizard are 1024-bit RSA keys. If you do not create and use SSL server certificates and SSH host keys with the APC Security Wizard, the Management Card generates 768-bit RSA keys.

Only APC server management and key management products can use server certificates, host keys, and CA root certificates created by the APC Security Wizard. These files will not work with products such as OpenSSL® and Microsoft IIS.

Create a Root Certificate & Server Certificates

Summary

Use this procedure if your company or agency does not have its own Certificate Authority and you do not want to use a commercial Certificate Authority to sign your server certificates.

Note

The public RSA key that is part of a certificate generated by the APC Security Wizard is 1024 bits. (The default key generated by the Management Card, if you do not use the Wizard, is 768 bits.)

- Create a CA root certificate that will be used to sign all server certificates to be used with Network Management Cards. During this task, two files are created.
  - The file with the **.p15** extension is an encrypted file which contains the Certificate Authority's private key and public root certificate. This file signs the server certificates.
  - The file with the **.crt** extension, which contains only the Certificate Authority's public root certificate. You load this file into each Web browser that will be used to access the Network Management Card so that the browser can validate the server certificate of the Management Card.
- Create a server certificate, which is stored in a file with a **.p15** extension. During this task, you are prompted for the CA root certificate that signs the server certificate.
- Load the server certificate onto the Network Management Card.
- For each Network Management Card that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the CA root certificate. Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC Network Management Card *utility* CD.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled "Step 1," select **CA Root Certificate** as the type of file to create.
4. Enter a name for the file that will contain the Certificate Authority's public root certificate and private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. On the screen labeled "Step 2," provide the information to configure the CA root certificate. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter an identifying name of your company or agency; use only alphanumeric characters, with no spaces.

Note

By default, a CA root certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.

Note The certificate's subject information and the certificate's issuer information should be identical.

7. The last screen verifies that the certificate has been created and instructs you on the next tasks.
   - This screen displays the location and name of the **.p15** file that you will use to sign the server certificates.
   - This screen also displays the location and name of the **.crt** file, which is the CA root certificate that you will load into the browser of each user who needs to access the Management Card.

Load the CA root certificate to your browser. Load the **.crt** file to the browser of each user who needs to access the Management Card.

See also See the help system of the browser for information on how to load the **.crt** file into the browser's certificate store (cache). Following is a summary of the procedure for Microsoft Internet Explorer.

1. Select **Tools**, then **Internet Options** from the menu bar.
2. On the **Content** tab in the **Internet Options** dialog box, click **Certificates** and then **Import**.
3. The Certificate Import Wizard will guide you through the rest of the procedure. The file type to select is X.509, and the CA Public Root Certificate is the **.crt** file created in the procedure Create a Root Certificate & Server Certificates.

Create an SSL Server User Certificate. Perform these steps. (Click **Next** to move from screen to screen.)

1. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
2. On the screen labeled Step 1, select **SSL Server Certificate** as the type of file to create.
3. Enter a name for the file that will contain the server certificate and the private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
4. Click the **Browse** button, and select the CA root certificate created in the procedure Create a Root Certificate & Server Certificates. The CA Root Certificate is used to sign the Server User Certificate being generated.
5. On the screen labeled Step 2, provide the information to configure the server certificate. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter the IP address or DNS name of the server (Network Management Card). Because the configuration information is part of the signature, it cannot be exactly the same as the information you provided when creating the CA root certificate; the information you provide in some of the fields must be different.

   Note: By default, a server certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate's unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.

Note

The information for every certificate must be unique. The configuration of a server certificate cannot be the same as the configuration of the CA root certificate. (The expiration date is not considered part of the unique configuration; some other configuration information must also differ.)

7. The last screen verifies that the certificate has been created and instructs you on the next task, to load the server certificate to the Network Management Card. It displays the location and name of the Server Certificate, which has a **.p15** file extension and contains the Management Card private key and public root certificate.

Load the server certificate to the Management Card. Perform these steps:

1. On the **Network** menu of the Web interface of the Network Management Card, select the **Web/SSL** option.
2. In the **SSL/TLS Server Certificate** section of the page, browse to the server certificate, the **.p15** file you created in the procedure Create a Root Certificate & Server Certificates. (The default is **C:\Program Files\American Power Conversion\APC Security Wizard**.)

Note

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Management Card. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Management Card. For SCP, the command to transfer a certificate named **cert.p15** to a Management Card with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\cert.p15
```

Create a Server Certificate and Signing Request

Summary

Use this procedure if your company or agency has its own Certificate Authority or if you plan to use a commercial Certificate Authority to sign your server certificates.

- Create a Certificate Signing Request (CSR).The CSR contains all the information for a server certificate except the digital signature. This process creates two output files:
  - The file with the **.p15** extension contains the Network Management Card's private key.
  - The file with the **.csr** extension contains the certificate signing request, which you send to an external Certificate Authority.
- When you receive the signed certificate from the Certificate Authority, import that certificate. Importing the certificate combines the **.p15** file containing the private key and the file containing the signed certificate from the external Certificate Authority. The output file is a new encrypted server certificate file with a **.p15** extension.
- Load the server certificate onto the Network Management Card.
- For each Network Management Card that requires a server certificate, repeat the tasks that create and load the server certificate.

The procedure

Create the Certificate Signing Request (CSR). Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC Network Management Card *utility* CD.

2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled “Step 1,” select **Certificate Request** as the type of file to create.
4. Enter a name for the file that will contain the Network Management Card’s private key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. On the screen labeled Step 2, provide the information to configure the certificate signing request (CSR) with the information that you want the signed server certificate to contain. The **Country** and **Common Name** fields are required; the other fields are optional. For the **Common Name** field, enter the IP Address or DNS name of the Network Management Card.

Note

By default, a server certificate is valid for 10 years from the current date and time, but you can edit the **Validity Period Start** and **Validity Period End** fields.

6. On the next screen, review the summary of the certificate. Scroll downward to view the certificate’s unique serial number and fingerprints. To make any changes to the information you provided, click **Back**, and revise the information.

Note

The certificate’s subject information and the certificate’s issuer information should be identical.

7. The last screen verifies that the certificate signing request has been created and displays the location and name of the file, which has a **.csr** extension.

8. Send the certificate signing request to an external Certificate Authority, either a commercial Certificate Authority or, if applicable, a Certificate Authority managed by your own company or agency.

See also

See the instructions provided by the Certificate Authority regarding the signing and issuing of server certificates.

Import the signed certificate. When the external Certificate Authority returns the signed certificate, perform these steps to import the certificate. This procedure combines the signed certificate and the private key into an SSL server certificate that you then upload to the Network Management Card. (Click **Next** to move from screen to screen.)

1. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
2. On the screen labeled Step 1, select **Import Signed Certificate**.
3. Browse to and select the signed server certificate that you received from the external Certificate Authority. The file has a **.cer** or **.crt** extension.
4. Browse to and select the file you created in step 4 of the task, Create the Certificate Signing Request (CSR). This file has a **.p15** extension, contains the Network Management Card's private key, and, by default, is located in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. Specify a name for the output file that will be the signed server certificate that you upload to the Management Card. The file must have a **.p15** extension.
6. Click **Next** to generate the server certificate. The certificate's **Issuer Information** on the summary screen confirms that the external Certificate Authority signed the certificate.

7. The last screen verifies that the certificate has been created and instructs you on the next task, to load the server certificate to the Network Management Card. It displays the location and name of the server certificate, which has a **.p15** file extension and contains the Management Card's private key and the public key obtained from the **.cer** or **.crt** file.

Load the server certificate to the Management Card. Perform these steps:

1. On the **Network** menu of the Web interface of the Network Management Card, select the **Web/SSL** option.
2. In the **SSL/TLS Server Certificate** section of the page, browse to the server certificate, the **.p15** file you created in the procedure Import the signed certificate. (The default location is **C:\Program Files\American Power Conversion\APC Security Wizard**.)

Note

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the server certificate to the Management Card. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Management Card. For SCP, the command to transfer a certificate named **cert.p15** to a Management Card with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\cert.p15
```

Create an SSH Host Key

Summary

This procedure is optional. If you select SSH encryption, but do not create a host key, the Network Management Card generates a 768-bit RSA key when it reboots. Host keys for SSH that are created with the APC Security Wizard are 1024-bit RSA keys.

- Use the APC Security Wizard to create a host key, which is encrypted and stored in a file with **.p15** extension.
- Load the host key onto the Management Card.

The procedure

Create the host key. Perform these steps. (Click **Next** to move from screen to screen.)

1. If the APC Security Wizard is not already installed on your computer, install it by running the installation program **APC Security Wizard.exe** from the APC Network Management Card *utility* CD.
2. On the Windows **Start** menu, select **Programs**, then **APC Security Wizard**, to start the Wizard program.
3. On the screen labeled Step 1, select **SSH Server Host Key** as the type of file to create.
4. Enter a name for the file that will contain the host key. The file name must have a **.p15** extension. By default, the file will be created in the installation folder **C:\Program Files\American Power Conversion\APC Security Wizard**.
5. Click **Next** to generate the Host Key
6. The summary screen displays the SSH version 1 and version 2 fingerprints, which are unique for each host key and identify the host key. After you load the host key onto the Management Card, you can

verify that the correct host key was uploaded by verifying that the fingerprints displayed here match the SSH fingerprints on the Management Card, as displayed by your SSH client program.

7. The last screen verifies that the host key has been created and instructs you on the next task, to load the host key to the Network Management Card. It displays the location and name of the host key, which has a **.p15** file extension.

Load the host key to the Management Card. Perform these steps:

1. On the **Network** menu of the Web interface of the Network Management Card, select the **Telnet/SSH** option.
2. In the **SSH User Host Key File** section of the page, browse to the host key, the **.p15** file you created in the procedure Create the host key. (The default location is **C:\Program Files\American Power Conversion\APC Security Wizard**.)
3. On the **SSH Host Key Fingerprint** section of the page, note the fingerprint for the version (or versions) of SSH you are using. Then log on to the Management Card through your SSH client program, and verify that the correct host key was uploaded by verifying that these fingerprints match the fingerprints that the client program displays.

Note

Alternatively, you can use FTP or Secure CoPy (SCP) to transfer the host key file to the Management Card. If you use FTP or SCP for the transfer, you must specify the correct location, **\sec**, on the Management Card. For SCP, the command to transfer a host key named **hostkey.p15** to a Management Card with an IP address of 156.205.6.185 would be:

```
scp cert.p15 apc@156.205.6.185:\sec\hostkey.p15
```

Troubleshooting

Management Card

Management Card access problems

See also

For problems that are not described here, see the troubleshooting flowcharts in *.\trouble* on the APC Network Management Card *utility* CD.

If the problem still persists, see Warranty and Service.

Problem	**Solution**
Unable to ping the Management Card	If the Management Card's Status LED is green, try to ping another node on the same network segment as the Management Card. If that fails, it is not a problem with the Management Card. If the Status LED is not green, or if the ping test succeeds, perform the following checks: • Verify that the Management Card is properly seated in the UPS or expansion chassis. • Verify all network connections. • Verify the IP addresses of the Management Card and the NMS. • If the NMS is on a different physical network (or subnetwork) from the Management Card, verify the IP address of the default gateway (or router). • Verify the number of subnet bits for the Management Card's subnet mask.

Problem	Solution
The terminal program cannot allocate the communications port when you try to configure the Management Card	Before you can use a terminal to configure the Management Card, you must shut down any application, service, or program using the communications port.
Cannot access the control console through a serial connection	Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.
Cannot access the control console remotely	• Make sure you are using the correct access method (Telnet or SSH). An Administrator can enable these access methods through the **Telnet/SSH** option of the **Network** menu. By default, Telnet is enabled. Enabling SSH automatically disables Telnet. • For Secure SHell (SSH), the Management Card may be creating a host key. The Management Card can take up to 5 minutes to create this host key, and SSH is not accessible during that time.
Cannot access the Web interface	• Verify that HTTP or HTTPS access is enabled. • Make sure you are specifying the correct URL — one that is consistent with the security system used by the Management Card. SSL requires **https**, not **http**, at the beginning of the URL. • Verify that you can ping the adapter. • Verify that you are using a Web browser that is supported for the Network Management Card. See Supported Web Browsers. • If the Network Management Card has just restarted and SSL security is being set up, the Management Card may be generating a server certificate. The Management Card can take up to 5 minutes to create this certificate, and the SSL/TLS server is not available during that time.

SNMP issues

The following table describes known SNMP problems:

Problem	Solution
Unable to perform a GET	• Verify the read (GET) community name. • Use the control console or Web interface to ensure that the NMS has access. See SNMP.
Unable to perform a SET	• Verify the read/write (SET) community name. • Use the control console or Web interface to ensure that the NMS has write (SET) access. See SNMP.
Unable to receive traps at the NMS	Query the **mconfigTrapReceiverTable** APC MIB OID to verify that the NMS IP address is listed correctly, and the community name defined for the NMS matches the community name in the table. If either is not correct, use SETs to the **mconfigTrapReceiverTable** OIDs, or use the control console or Web interface to correct the trap receiver definition. See SNMP.
Traps received at an NMS are not identified	See your NMS documentation to verify that the traps are properly integrated in the alarm/trap database.

Synchronization problems

Problem	Solution
A Synchronized Control Group member does not participate in a synchronized action.	Make sure the group member's status is set to **Enabled**. Also check the group member's battery capacity, if the synchronized action required UPSs to turn on.
An attempt to add a member to a Synchronized control group fails.	The **Multicast IP Address**, **Synchronized Control Group Number**, and firmware version must match those of other members of the group.

How to Export Configuration Settings

Retrieving and Exporting the .ini file

Summary of the procedure

As an Administrator, you can retrieve a dynamically generated .ini file of a Network Management Card's current configuration and export that file to another Network Management Card or to multiple Network Management Cards.

1. You configure a Network Management Card to have the settings you want to export.
2. You retrieve the .ini file from that Management Card.
3. You then customize the .ini file (to change at least the TCP/IP settings) and make a copy to export.
4. You use any of the file transfer protocols supported by the Network Management Card to transfer the copied file to one or more additional Management Cards. (To transfer the file to multiple Management Cards simultaneously, write an FTP or SCP script that repeats the steps for transferring the file to a single Management Card.)
5. Each receiving Network Management Card stores the file temporarily in its flash memory, uses it to reconfigure its own Management Card settings, and then deletes the file.

Contents of the .ini file

The config.ini file that you retrieve from a Network Management Card contains the following:

- *section headings*, which are category names enclosed in brackets ([ ]), and under each section heading, *keywords,* which are labels describing specific Management Card settings.

  Note: Only section headings and keywords supported for the specific device associated with the Management Card from which you retrieve the file are included.

- Each keyword is followed by an equals sign and the current *value* for that parameter's setting, either the default value (if the value has not been specifically configured) or the configured value.
  - The `Override` keyword, with its default value, prevents one or more keywords and their device-specific values from being exported.
    - In the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the Management Card) blocks the exporting of the values for the keywords `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.
    - In the UPS section, the default value for `Override` (the UPS serial number) blocks the exporting of the value for the `RatedOutputVoltage` keyword. (`RatedOutputVoltage` and its value are included only in the .ini file only if the output voltage of the UPS is configurable.)
  - You must edit the section `[SystemDate/Time]` if you want to set the system date and time of a receiving Management Card or cause that Management Card to use an NTP Server to set its date and time.

    See Customizing for configuration guidelines for date and time settings.

Detailed procedures

Use the following procedures to retrieve the settings of one Network Management Card and export them to one or more other Network Management Cards.

Retrieving. To set up and retrieve an .ini file to export:

1. Configure a Management Card with the settings you want to export.

   Note: To avoid errors, configure the Management Card by using its Web interface or control console whenever possible. Directly editing the .ini file risks introducing errors.

2. Use FTP to retrieve the file config.ini from the Management Card you configured:

   a. Open a connection to the Management Card, using its IP Address. For example:

   ```
   ftp> open 158.165.2.132
   ```

   b. Log on, using the Administrator user name and password configured for the Management Card.

   c. Retrieve the config.ini file containing the Management Card's current settings:

   ```
   ftp> get config.ini
   ```

   The file is written to the folder from which you launched FTP.

See also: To create batch files and use an APC utility to retrieve configuration settings from multiple Management Cards and export them to other Management Cards, see *Release Notes: ini File Utility, version 1.0* (**.\doc\en\ininotes.pdf**) on the APC Network Management Card *utility* CD.

Customizing. You must customize the file to change at least the TCP/IP settings before you export it.

1. Use a text editor to customize the file.
   - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
   - To define values, opening and closing quotation marks are optional, except to enclose values that contain leading or trailing spaces or values which are already enclosed in quotation marks. (Leading or trailing spaces not within the opening and closing quotation marks are ignored.)
   - To export a specific system date and time or any scheduled events, you must configure the values directly in the .ini file.
     - To export a specific system time, export only the configured `[SystemDate/Time]` section as a separate .ini file. (The time necessary to export a large file would cause the configured time to be significantly inaccurate.)
     - For greater accuracy, if the Network Management Cards receiving the file can access a Network Time Protocol (NTP) Server, set the value for the `NTPEnable` keyword as follows:

       ```
       NTPEnable=enabled
       ```
   - Add comments about changes that you made. The first printable character of a comment line must be a semicolon (`;`).
2. Copy the customized file to another file name in the same folder:
   - The copy, which you will export to other Management Cards, can have any file name up to 64 characters and must have the .ini file suffix.
   - Retain the original customized file for future use. **The file that you retain is the only record of your comments.** They are removed automatically from the file that you export.

Exporting the file to a single Management Card. To export the .ini file to another Network Management Card, use any of the file transfer protocols supported by Network Management Cards (including FTP, FTP Client, SCP, and TFTP). The following example uses FTP:

1. From the folder containing the customized .ini file and its copy, use FTP to log in to the Management Card to which you are exporting the .ini file. For example:

   ```
   ftp> open 158.165.4.135
   ```

2. Export the copy of the customized .ini file. The receiving Management Card accepts any file name that has the .ini suffix, is no more than 64 characters in length, and is exported to its root directory.

   ```
   ftp> put filename.ini
   ```

Exporting the file to multiple Management Cards. To export the .ini file to multiple Network Management Cards:

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single Management Card.
- Use a batch processing file and the APC .ini file utility.

See also

To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* (**.\doc\en\ininotes.pdf**) on the APC Network Management Card *utility* CD.

The Upload Event and Error Messages

The event and its error messages

The following system event occurs when the receiving Network Management Card completes using the .ini file to update its settings.

```
Configuration file upload complete, with number valid values
```

This event has no default severity level.

If a keyword, section name, or value is invalid, the event text is extended to include notification of the following errors.

Note

The export to and the subsequent upload by the receiving Management Card succeeds even if there are errors.

Event text	**Description**
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number.*	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number*.	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, the Management Card stores and processes what it can, but ignores what it cannot. Reduce the size of the file, or divide it into two files, and try uploading again.

Messages in config.ini

A device associated with the Management Card from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the device (such as a UPS or Integrated Environmental Monitor) is not present or, for some other reason, is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values. For example:

```
UPS not discovered

IEM not discovered
```

If you did not intend to export the configuration of the device as part of the .ini file import, ignore these messages.

Errors generated by overridden values

The `Override` keyword and its value will generate error messages in the event log when it blocks the exporting of values.

See Contents of the .ini file for information about which values are overridden.

The overridden values are device-specific and not appropriate to export to other Management Cards. Therefore, you can ignore these error messages. To prevent these error messages from occurring, you can delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Using the APC Device IP Configuration Wizard

On Windows operating systems, instead of using the preceding procedure for exporting .ini files, you can choose to update the basic TCP/IP settings of Management Cards by using the APC Device IP Configuration Wizard.

SeeAPC Device IP Configuration Wizard for a detailed description of how to discover and configure unconfigured Network Management Cards remotely over your TCP/IP network or configure or reconfigure a Network Management Card through a direct connection from the serial port of your computer to the Network Management Card.

APC Device IP Configuration Wizard

Purpose and Requirements

Purpose: configure basic TCP/IP settings

You can use the APC Device IP Configuration Wizard to configure the basic TCP/IP settings (IP address, subnet mask, and default gateway) of the following:

- Network Management Cards
- Devices that contain embedded Network Management Cards

Using the Wizard, you can configure the basic TCP/IP settings of installed or embedded Network Management Cards in either of the following ways:

- Automatically discover and configure unconfigured Network Management Cards remotely over your TCP/IP network.
- Configure or reconfigure a Network Management Card through a direct connection from the serial port of your computer to the device that contains the card.

Note: The Wizard can discover and configure Network Management Cards only if they are on the same network segment as the computer that is running the Wizard.

System requirements

The Wizard runs on Windows NT®, Windows 2000, Windows 2003, and Windows XP Intel-based workstations.

Install the Wizard

Automated installation

If autorun is enabled on your CD-ROM drive, the installation program starts automatically when you insert the CD.

Manual installation

If autorun is not enabled on your CD-ROM drive, run **setup.exe** in the Wizard directory on the CD, and follow the on-screen instructions.

You can also download the latest version of the APC Device IP Configuration Wizard from the APC web site, **www.apc.com** and run **setup.exe** from the folder to which you downloaded it.

Use the Wizard

Launch the Wizard

The installation creates a shortcut link in the **Start** menu that you can use to launch the Wizard.

Configure the basic TCP/IP settings remotely

Prepare to configure the settings. Before you run the Wizard, be sure that you have the information you will need during the configuration procedure:

1. Contact your network administrator to obtain valid TCP/IP settings to use.
2. If you are configuring multiple unconfigured Network Management Cards, obtain the MAC address of each one so that you can identify each Network Management Card that the Wizard discovers. (The Wizard displays the MAC address for a discovered card on the same screen on which you then enter the TCP/IP settings.)

- For Network Management Cards that you install, the MAC address is on a label on the bottom of the card.
- For embedded Network Management Cards, the MAC address is on a label on the device containing the card — for example, usually on the side of a device that you mount in a rack.

  You can also obtain the MAC address from the Quality Assurance slip that came with the Network Management Card or with the device containing an embedded Network Management Card.

Run the Wizard to perform the configuration. To discover and configure, over the network, installed or embedded Network Management Cards that are not configured:

1. From the **Start** menu, launch the Wizard. The Wizard automatically detects the first Network Management Card that is not configured.
2. Select **Remotely (over the network)**, and click **Next >**.
3. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the unconfigured Network Management Card identified by the MAC address at the top of the screen. Then click **Next >**.
4. On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the device that contains the Network Management Card after you transmit the card's settings.
5. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
6. The Wizard searches for another installed or embedded but unconfigured Network Management Card. If it finds one, it displays the screen with data entry boxes for the TCP/IP settings of that card.
   - To skip configuring the card whose MAC address is currently displayed, click **Cancel**.
   - To configure the TCP/IP settings of the next card, repeat this procedure beginning at step 4.

Configure or reconfigure the TCP/IP settings locally

To configure a single Network Management Card through a serial connection:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. Connect the serial configuration cable that came with the Network Management Card or with the device that contains an embedded Network Management Card.

   a. Connect one end to an available communications port on your computer. Make sure no other application is using the port.
   b. Connect the other end to the serial port of the card or device.
3. From the **Start** menu, launch the Wizard application.
   – If the Network Management Card is not configured, wait for the Wizard to detect it.
   – If you are assigning basic TCP/IP settings serially to a Network Management Card, click **Next>** to move to the next screen.
4. Select **Locally (through the serial port)**, and click **Next >**.
5. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the Network Management Card. Then click **Next >**.
6. On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the device that contains the Network Management Card after you transmit the card's settings.
7. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
8. If you selected **Start a Web browser when finished** in step 6, you can now configure other parameters through the Web interface of the card or device.

File Transfers

Introduction

Overview

The Network Management Card automatically recognizes binary firmware files. Each of these files contains a header and one or more Cyclical Redundancy Checks (CRCs) to ensure that the data contained in the file is not corrupted before or during the transfer operation.

When new firmware is transmitted to the Management Card, the program code is updated and new features become available.

This chapter describes how to transfer firmware files to Network Management Cards.

Note

To transfer a firmware file to a Management Card, see Upgrading Firmware.

To verify a file transfer, see Verifying Upgrades and Updates.

Upgrading Firmware

Benefits of upgrading firmware

Upgrading the firmware on the Network Management Card has the following benefits:

- New firmware has the latest bug fixes and performance improvements.
- New features become available for immediate use.
- Keeping the firmware versions consistent across your network ensures that all Network Management Cards support the same features in the same manner.

Firmware files (Network Management Card)

A firmware version consists of two modules: An APC Operating System (AOS) module and an application module.

The APC Operating System (AOS) and application module files used with the Network Management Card share the same basic format:

`apc_hw0x_type_version.bin`

- `apc`: Indicates that this is an APC file.
- `hw0x`: Identifies the version of the Network Management Card that will run this binary file.
- *`type`*: Identifies whether the file is for the APC Operating System (AOS) or the application module (APP) for the Network Management Card.
- *`version`*: The version number of the application file. For example, a code of 261 would indicate version 2.6.1.
- `bin`: Indicates that this is a binary file.

Obtain the latest firmware version

Automated upgrade tool for Microsoft Windows systems. An automated self-extracting executable tool combines the firmware modules that you need to automate your upgrades on any supported Windows operating system

- The version of the tool on the APC Network Management Card *utility* CD will upgrade your device to the latest AOS and application modules available when the CD was released.
- If a later firmware upgrade is available, you can obtain an updated version of the tool at no cost from the support section of the APC web site **www.apc.com/tools/download**. At this Web page, find the latest firmware release for your APC product (in this case, your Management Card) and download the automated tool, not the individual firmware modules.

If the AOS firmware module you already have is a 1.*x*.*x* version, the executable tool must perform two consecutive upgrades:

- The first upgrade is from version 1.*x*.*x* to the latest available 2.0.*x* version of the AOS firmware module.
- The second upgrade is from the 2.0.*x* version to the most recently released version of the AOS module.

The tool therefore contains firmware modules for both upgrades.

Each upgrade tool is specific to an APC product type. Do not use the tool from one product CD to upgrade firmware of a different APC product. If you use a version of the tool from the APC Web site, make sure that you use the upgrade tool that corresponds with your APC product type.

Manual upgrades, primarily for Linux systems. If all computers on your network are running Linux, you must upgrade the firmware of your Management Cards manually, i.e., by using the separate APC firmware modules (AOS module and application module).

If you have a networked computer running a supported Microsoft Windows operating system on your network, you can use the tool described in Automated upgrade tool for Microsoft Windows systems to upgrade the firmware of a Network Management Card automatically over the network. This tool automates the entire upgrade process, even if your current firmware is a 1.*x.x* version.

Note

When performing a manual upgrade, not using the automated tool, you cannot upgrade the AOS firmware module of any APC device directly from firmware version 1.*x.x* to firmware version 2.1.0 or later. The upgrade attempt will fail. You must first upgrade to the latest availaible 2.0.*x* version of the AOS module and then to the later version.

You can obtain the individual firmware modules you need for a manual firmware upgrade from the support section of the APC web site **www.apc.com/tools/download**.

Firmware file transfer methods

To upgrade the firmware of a Network Management Card:

- From a networked computer running a Microsoft Windows operating system, you can use the automated firmware upgrade tool on your CD or downloaded from the APC Web site.
- From a networked computer on any supported operating system, you can use FTP or SCP to transfer the individual AOS and application firmware modules.
- For a Network Management Card that is not on your network, you can use XMODEM through a serial connection to transfer the individual AOS and application firmware modules from your computer to the Network Management Card.

Note

When you transfer individual firmware modules and do not use the automated firmware upgrade tool to upgrade the firmware for a Management Card, you must transfer the APC Operating System (AOS) module to the Management Card before you transfer the application module.

For more information about the firmware modules, see Firmware files (Network Management Card).

Use FTP or SCP to upgrade one Management Card

Instructions for using FTP. For you to be able to use FTP to upgrade a single Network Management Card over the network:

- The Network Management Card must be connected to the network.
- The FTP server must be enabled at the Network Management Card.
- The Network Management Card must have its TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway** addresses) configured.

To use FTP to upgrade the Management Card:

1. Open an MS-DOS command prompt window on a computer that is connected to the network. Go to the directory that contains the firmware upgrade files, and list the files. For the directory `C:\apc`, the commands would be those shown in **bold**:

   ```
   C:\>cd\apc
   C:\apc>dir
   ```

   Files listed for a Network Management Card, for example, might be the following:

   ```
   –apc_hw02_aos_261.bin
   –apc_hw02_app_261.bin
   ```

2. Open an FTP client session:

   ```
   C:\apc>ftp
   ```

3. Type `open` and the Network Management Card's IP address, and press ENTER. If the **Port** setting for **FTP Server** in the **Network** menu has changed from its default of **21**, you must use the non-default value in the FTP command.

   a.For some FTP clients, use a colon to add the port number to the end of the IP address.

b. For Windows FTP clients, separate the port number from the IP address by a space. For example, if the Management Card's **FTP Server Port** setting has been changed from its default of **21**, such as to **21000**, you would use the following command for a Windows FTP client transferring a file to a Management Card with an IP address of 150.250.6.10.

```
ftp> open 150.250.6.10 21000
```

4. Log on using the Administrator user name and password. (**apc** is the default for both.)
5. Upgrade the AOS. For example:

```
ftp> bin
ftp> put apc_hw02_aos_261.bin
```

6. When FTP confirms the transfer, type **quit** to close the session.
7. Wait 20 seconds, and then repeat step 2 through step 6, but in step 6, use the application module file name instead of the AOS module.

Instructions for using SCP. To use Secure CoPy (SCP) to upgrade the firmware for one Management Card:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the Management Card. The following example assumes a Management Card IP address of 158.205.6.185, and an AOS module of **apc_hw02_aos_261.bin**.)

```
scp apc_hw02_aos_261.bin apc@158.205.6.185:apc_hw02_aos_261.bin
```

3. Use a similar SCP command line, with the name of the application module instead of the AOS module, to transfer the application module to the Management Card.

How to upgrade multiple Management Cards

Export configuration settings. You can create batch files and use an APC utility to retrieve configuration settings from multiple Management Cards and export them to other Management Cards.

See also

See *Release Notes: ini File Utility, version 1.0* (**.\doc\en\ininotes.pdf**) on the APC Network Management Card *utility* CD.

Use FTP or SCP to upgrade multiple Management Cards. To upgrade multiple Network Management Cards using an FTP client or using SCP, write a script which automatically performs the procedure. For FTP, use the steps in Use FTP or SCP to upgrade one Management Card.

Use XMODEM to upgrade one Management Card

Note

You cannot upgrade the AOS firmware module of any APC device directly from firmware version 1.*x.x* to 2.1.0 or later. The upgrade attempt will fail.

To upgrade the AOS firmware module of an APC device from version 1.*x.x* to 2.1.0 or later, first upgrade the module to the latest available version 2.0.*x* AOS firmware module. Then upgrade it again, this time from version 2.0.*x* to the 2.*x.x* version you want.

If your APC device is running a 2.0.*x* of the AOS firmware module already, you can upgrade directly to version 2.1.0 or a later version.

To use XMODEM to upgrade the firmware for a single Network Management Card that is not on the network:

1. Obtain the individual firmware modules (the AOS module and the application module) from the support section of the APC web site **www.apc.com/tools/download**.
2. Select a serial port at the local computer and disable any service which uses that port.
3. Connect the smart-signaling cable that came with the Management Card to the selected port and to the serial port at the Management Card.
4. Run a terminal program (such as HyperTerminal®), and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control, and save the changes.
5. Press ENTER to display the **User Name** prompt.
6. Enter your Administrator user name and password. The default for

both is **apc**.

7. Start an XMODEM transfer:

   a. Select option 3—**System**

   b. Select option 4—**File Transfer**

   c. Select option 2—**XMODEM**

   d. Type `Yes` at the prompt to continue with the transfer.

8. Select the appropriate baud rate. A higher baud rate causes faster firmware upgrades. Also, change the terminal program's baud rate to match the one you selected, and press ENTER.

9. From the terminal program's menu, select the binary AOS file to transfer via XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600. The Management Card will automatically restart.

10. Repeat **step 3** through **step 8** to install the application module. In **step 8**, substitute the application module file name for the AOS module file name.

For information about the format used for application modules, see Firmware files (Network Management Card).

Verifying Upgrades and Updates

Overview

To verify that the firmware upgrade was successful, see the **Last Transfer Result** message, available through the **FTP Server** option of the **Network** menu (in the control console only), or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last Transfer Result codes

Code	Description
Successful	The file transfer was successful.
Result not available	There are no recorded file transfers.
Failure unknown	The last file transfer failed for an unknown reason.
Server inaccessible	The TFTP or FTP server could not be found on the network.
Server access denied	The TFTP or FTP server denied access.
File not found	The TFTP or FTP server could not locate the requested file.
File type unknown	The file was downloaded but the contents were not recognized.
File corrupt	The file was downloaded but at least one CRC was bad.

You can also verify the versions of the upgraded APC Operating System (AOS) and application modules by using the **About System** option in the **System** menu of the control console or in the **Help** menu of the Web interface, or by using an SNMP GET to the MIB II **sysDescr** OID.

Product Information

Warranty and Service

Limited warranty

APC warrants the Network Management Card to be free from defects in materials and workmanship for a period of two years from the date of purchase. Its obligation under this warranty is limited to repairing or replacing, at its own sole option, any such defective products. This warranty does not apply to equipment that has been damaged by accident, negligence, or misapplication or has been altered or modified in any way. This warranty applies only to the original purchaser.

Warranty limitations

Except as provided herein, APC makes no warranties, expressed or implied, including warranties of merchantability and fitness for a particular purpose. Some jurisdictions do not permit limitation or exclusion of implied warranties; therefore, the aforesaid limitation(s) or exclusion(s) may not apply to the purchaser.

Except as provided above, in no event will APC be liable for direct, indirect, special, incidental, or consequential damages arising out of the use of this product, even if advised of the possibility of such damage.

Specifically, APC is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, costs of substitutes, claims by third parties, or otherwise. This warranty gives you specific legal rights and you may also have other rights, which vary according to jurisdiction.

Obtaining service

To obtain support for problems with your Network Management Card:

1. Note the serial number and date of purchase. For a separately shipped Management Card, the serial number is on the card itself. For a UPS with a pre-installed or embedded card, note the serial number of the UPS itself.
2. Contact Customer Support at a phone number listed under APC Worldwid Customer Support at the end of this manual. A technician will try to help you solve the problem by phone.
3. If you must return the product, the technician will give you a return material authorization (RMA) number. If the warranty expired, you will be charged for repair or replacement.
4. Pack the unit carefully. The warranty does not cover damage sustained in transit. Enclose a letter with your name, address, RMA number and daytime phone number; a copy of the sales receipt; and a check as payment, if applicable.
5. Mark the RMA number clearly on the outside of the shipping carton.
6. Ship by insured, prepaid carrier to the address provided by the Customer Support technician.

Caution

THE NETWORK MANAGEMENT CARD IS SENSITIVE TO STATIC ELECTRICITY. WHEN HANDLING THE MANAGEMENT CARD, TOUCH ONLY THE END PLATE WHILE USING ONE OR MORE OF THESE ELECTROSTATIC-DISCHARGE DEVICES (ESDS): WRIST STRAPS, HEEL STRAPS, TOE STRAPS, OR CONDUCTIVE SHOES.

Recycling the Battery

The Network Management Card contains a removable, lithium coin-cell battery. When discarding this battery, you must follow local rules for recycling.

Life-Support Policy

General policy

American Power Conversion (APC) does not recommend the use of any of its products in the following situations:

- In life-support applications where failure or malfunction of the APC product can be reasonably expected to cause failure of the life-support device or to affect significantly its safety or effectiveness.
- In direct patient care.

APC will not knowingly sell its products for use in such applications unless it receives in writing assurances satisfactory to APC that (a) the risks of injury or damage have been minimized, (b) the customer assumes all such risks, and (c) the liability of American Power Conversion is adequately protected under the circumstances.

Examples of life-support devices

The term *life-support device* includes but is not limited to neonatal oxygen analyzers, nerve stimulators (whether used for anesthesia, pain relief, or other purposes), autotransfusion devices, blood pumps, defibrillators, arrhythmia detectors and alarms, pacemakers, hemodialysis systems, peritoneal dialysis systems, neonatal ventilator incubators, ventilators (for adults and infants), anesthesia ventilators, infusion pumps, and any other devices designated as “critical” by the U.S. FDA.

Hospital-grade wiring devices and leakage current protection may be ordered as options on many APC UPS systems. APC does not claim that units with these modifications are certified or listed as hospital-grade by APC or any other organization. Therefore these units do not meet the requirements for use in direct patient care.

Specifications

Electrical

Item	Specification
Acceptable input voltage	19-30 VDC
Maximum total current draw	110 mA

Physical

Item	Specification
Size (H × W × D)	1.46 × 4.75 × 4.3 in (3.7 ×12.1 ×10.9 cm)
Weight	.25 lb (.11 kg)
Shipping weight	.8 lb (.36 kg)

Index

APC Worldwide Customer Support

Customer support for this or any other APC product is available at no charge in any of the following ways:

- Visit the APC Web site to access documents in the APC Knowledge Base and to submit customer support requests.
  - **www.apc.com** (Corporate Headquarters)

    Connect to localized APC Web sites for specific countries, each of which provides customer support information.
  - **www.apc.com/support/**

    Global support searching APC Knowledge Base and using e-support.
- Contact an APC Customer Support center by telephone or e-mail.
  - Regional centers:

Direct InfraStruXure Customer Support Line	(1)(877)537-0607 (toll free)
APC headquarters U.S., Canada	(1)(800)800-4272 (toll free)
Latin America	(1)(401)789-5735 (USA)
Europe, Middle East, Africa	(353)(91)702000 (Ireland)
Japan	(0) 35434-2021
Australia, New Zealand, South Pacific area	(61) (2) 9955 9366 (Australia)

  - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

Contact the APC representative or other distributor from whom you purchased your APC product for information on how to obtain local customer support.

USER'S GUIDE
network management card

Copyright

The Network Management Card is certified for use with APC InfraStruXure™ systems.

990-0385E-001 **07/2004**